# System Area Manager

V4.55

User Manual

August 2014

© 2014 SyAM Software, Inc.
All rights reserved. SyAM Software and the SyAM Software logo are trademarks of SyAM Software, Inc.
All other trademarks are the property of their respective owners.

Information contained in this document is assumed to be accurate at the time of publishing. SyAM Software reserves the right to make changes to the information contained in this document at any time without notice.

For additional information, sales, or technical support, contact SyAM Software

www.syamsoftware.com

# Table of Contents


Introduction ..... 4
SyAM Software Modules ..... 5
Compatibility ..... 5
System Requirements ..... 5
Browser Requirements ..... 5
Chapter 1: Installation and Configuration ..... 6
Firewall Security ..... 6
Chapter 2: Logging In ..... 7
Ending the Session ..... 8
Chapter 3: The SyAM System Area Manager User Interface ..... 9
Interface Layout ..... 9
Health Colors ..... 11
Icons ..... 11
Filter by, Grouping and Sorting Options for the Management Tree ..... 15
Chapter 4: License Management ..... 18
Chapter 5: Remote Management ..... 20
System State ..... 20
Wake on LAN ..... 21
Remote Console ..... 21
AMT (Intel® Active Management Technology) ..... 25
IPMI Event Log ..... 34
IPMI Over LAN ..... 36
DASH (Desktop and Mobile Architecture for System Hardware) ..... 38
Chapter 6: Central Event Logging ..... 49
Event Filtering ..... 49
Viewing Events ..... 51
Deleting Events from the Event Log ..... 52
Chapter 7: Central Reporting ..... 53
Report Types ..... 53
Report Filtering ..... 54
Application Summary Report ..... 55
Asset Details Report ..... 57
Asset List Report ..... 60
Asset Summary Report ..... 61
Operating System Summary Report ..... 63
User Audit Report ..... 64
Local Alert Report ..... 66
Application Utilization Report ..... 68
Power Hours Summary Report ..... 70
Power Hours Detail Report ..... 72
Chapter 8: Registering With Site Manager ..... 74
Chapter 9: Configuring System and Central Alerts ..... 75
Monitored Sensor Types ..... 76
Notification Settings ..... 78
Notification Settings – Configuring email alerting ..... 80
Local Alerting ..... 80
Central Alert Matrix ..... 81
Integration into Enterprise Frameworks ..... 83
Chapter 10: Accessing System Information ..... 84
System Detail Tab ..... 84
Power Management Tab ..... 87
Hardware Detail Tab ..... 91
Network Detail Tab ..... 92
Storage Detail Tab ..... 93
Software Details Tab ..... 99
Chapter 11: Configuring Platform Event Trap Support ..... 107
Chapter 12: Managing Users and Groups ..... 109
Chapter 13: Data Center Management ..... 113
Chapter 14: Contact Details & Glossary ..... 116

# Introduction

SyAM Software provides a comprehensive, simple to use set of system management products for servers, desktops, notebooks and tablets. Each product has features specific to their relevant system's capabilities and functions, as well as a large number of common features. Their user interfaces are identical.

The products enable several IT benefits. Among them are predictive alerting to pending failures, system configuration, unattended monitoring and alerting, remote management, and reporting. The products dynamically discover the hardware and software operating environment, and manage all physical environmental sensors available and operating system resources. Users can view them and be alerted if they exceed their thresholds.

There are two levels of system management. System Client software provides a single system view. System Area Manager provides a unified view of all of your systems, and also provides more comprehensive features.

The System Client management products are:

- Server System Client
- Desktop System Client
- Notebook System Client
- Tablet System Client

The Central Management product is:

- System Area Manager

This user manual describes the System Area Manager software. The following sections will describe the product functionality of the System Area Manager itself, and also explain how using the System Area Manager to manage other systems unlocks features in those systems.

# SyAM Software Modules

System Area Manager consists of two products:

- **System Area Manager – Server –** Provides the ability to manage Servers, Desktops and Notebook platforms running the System Client.
- **System Area Manager – Desktop –** Provides the ability to manage Desktops and Notebook platforms running the System Client.

These products can be installed on any Intel architecture x86/x64 platform running one of the supported operating systems.

# Compatibility

| ***Operating System*** | ***System Area Manager - Server*** | ***System Area Manager - Desktop*** |
|---|---|---|
| *Windows 2012 Server* | ■ | |
| *Windows 2008 R2 Server* | ■ | |
| *Windows 2008 Server* | ■ | |
| *Windows 8* | ■ | ■ |
| *Windows 7 Professional/Ultimate* | ■ | ■ |

# System Requirements

- 1GB Disk space
- 2GB Memory (4GB recommended)

# Browser Requirements

- Internet Explorer 7, 8, 9
- Mozilla Firefox

# Chapter 1: Installation and Configuration

1. Load the SyAM Software CD and from the menu choose the product version you wish to install, or double click the downloaded SyAM executable. Then just follow the Install Wizard instructions.
2. Choose the language of the user interface.
3. Choose the destination folder. This cannot contain any spaces in the name.
4. Do not change the RMI port default value of 10999 unless you know that port number is already in use.
5. To enable security through 128-bit data encryption from the SyAM Server Web Server to the browser, choose the SSL option. (default=No)
6. After the installation has finished, the SyAM services will start and dynamically discover and configure your system's monitoring environment.

## Firewall Security

The following ports must be opened if you are using a firewall on your Linux system. They are automatically opened on Windows operating systems during the installation.

- 3894 – Used for Agent management service
- 3895 – Used for Central management service
- 3930 – Used for Web server service
- 5800 – Used for Remote Console access from System Area Manager
- 5900 – Used for Remote Console access from System Area Manager
- 58900 – AMT SOL – Session #1
- 58901 – AMT SOL – Session #2
- 58902 – AMT SOL – Session #3

## Uninstalling System Area Manager (Windows)

**To remove System Area Manager from the Windows system:**

1. In Control Panel, select Programs and Features – Uninstall or change a program.
2. Highlight SyAM System Area Manager and select Uninstall. You will be prompted to confirm this action.
3. Following removal, if System Area Manager is to be reinstalled, a system restart is required.

# Chapter 2: Logging In

Open a supported web browser on any system with access to the server where System Area Manager is installed. In the URL bar, enter:

http://IPADDRESS:3930 *or* http://MACHINENAME:3930

Example: http://192.168.1.19:3930

Example: http://FILESERVER:3930

**If you enabled SSL during installation, you are required to type "https" instead of "http":**

Example: https://IPADDRESS:3930 or https://MACHINENAME:3930

**This will bring you to the login screen.**

The SyAM web server requests the operating system to log you in, using an account that is already in place on your system. To login you must satisfy the following conditions:

**For standalone systems (not in a Windows domain)**

- The user name and password must be valid on the system you are logging into.
- The user must have Administrator rights on the system.

**For systems within a Windows domain**

- The user name and password must be valid in the domain.
- The user must have "Domain Admin" rights within the Windows domain.
- A valid domain name for the system must be entered in the Domain field.

The first user logging into a newly installed System Area Manager is added to the Administrators group, with all privileges. To learn about adding more users, and changing user privileges, please refer to the chapter entitled Managing Users and Groups.

**Ending the Session**
When you have completed your management session, choose the Log Out button on the main header bar. Successful logout returns you to the login screen.

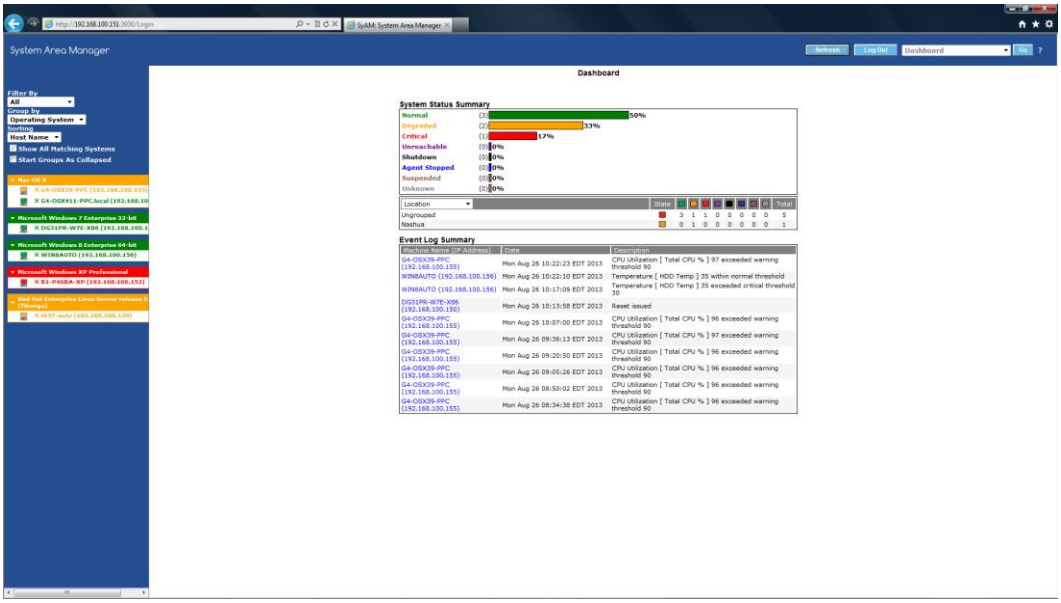
For added security you will be logged out automatically after 30 minutes of inactivity. A message box will appear on screen if you are using Internet Explorer to let you know that you need to log back in. If you are browsing with Firefox you will be logged out and returned to the login screen.

# Chapter 3: The SyAM System Area Manager User Interface

*SyAM System Area Manager provides administrators with the ability to manage a set of systems from a single user interface.*

## Interface Layout

The structure of the interface is identical whether you are using System Area Manager Server or Desktop. All of the systems being managed are represented in the tree on the left hand side. Detailed information about a specific system being accessed is presented on the main right hand side.

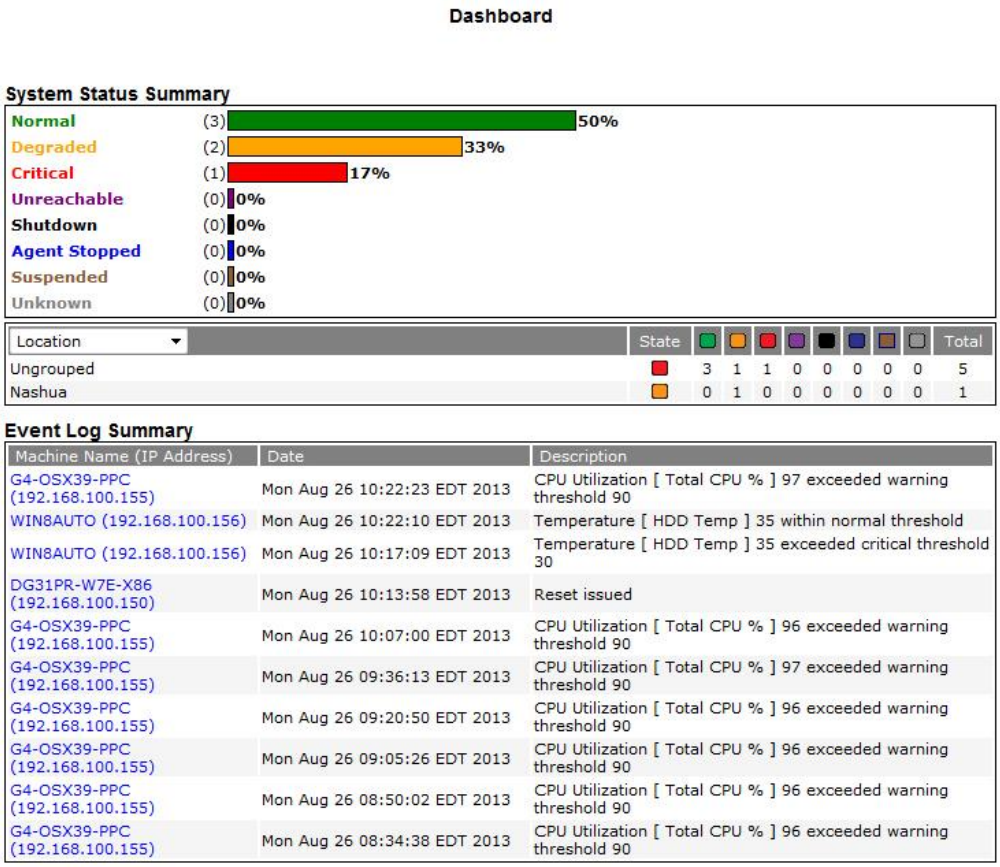



### Header Bar

The header bar has function buttons for Refresh and Log Out, a question-mark icon for Online Help, and a drop down menu for the central management functions: Dashboard, Add Managed Systems, Central Alert Matrix, Event Log, Report, License Management, Site Manager Registration and Version.

### Dashboard

The Dashboard provides the user with a chart showing the state of their managed systems. It displays the systems by the chosen grouping and (optionally) displays the last ten events that have occurred.




You can change the view of the system status summary by clicking on the down arrow and selecting the appropriate logical group.

To sort the management tree to display only a specific set of systems click on the status chart or the column and it will refresh the management tree with that filter by status.

Enabling the Event Log Summary option displays a list of recent events. Each entry has a Machine Name link to display system information.

**The Dashboard will automatically refresh every 5 minutes.**

You can configure the dashboard refresh time and can enable/disable showing the event log summary by editing the file syam.properties which is contained in this folder: C:\SyAM\Jetty\syam\webapps\root\WEB-INF\

**tree_refresh=15** Number of minutes between tree refreshes. This modification requires the SyAM Web Server service to be restarted
**dashboard_refresh=5** Number of minutes between dashboard refreshes. This modification requires the SyAM Web Server service to be restarted
**showDashboardEvents=false** By changing this to true the event log summary will be shown. This modification will take immediate effect and does not require the SyAM Web Server service to be restarted.

## Health Colors

In order to quickly identify and correct system problems, System Area Manager uses a consistent color scheme to represent the health and functionality of systems and their components. These colors can be seen in every level of monitoring, from the instance of the component to the component category and section. The health of each monitored system is updated on a regular interval. Any change in the status of the system will cause a change in the health color. The health color will remain in the changed state until the issue is resolved.

| | |
|---|---|
| | ***Green = Fully Functional*** |
| | *Amber = Warning* |
| | *Red = Critical* |
| | *Grey = System state pending, currently unknown* |
| | *Purple = System is no longer responding* |
| | *Blue = Agent service has been manually shut down* |
| | *Black = System has been shut down* |
| | *Brown = System power state has been suspended* |

## Icons

There are four icons that represent the type of SyAM System Client software running on the managed system.

| | |
|---|---|
| | *Server System Client* |
| | *Desktop System Client* |
| | *Notebook System Client* |
| | *Tablet System Client* |

# Adding Systems to the Management Tree

Systems must be added to the Management Tree before they can be managed centrally through the System Area Manager.

You can only add systems that are running the SyAM System Client, and may only add those systems up to the limit set by your license key.

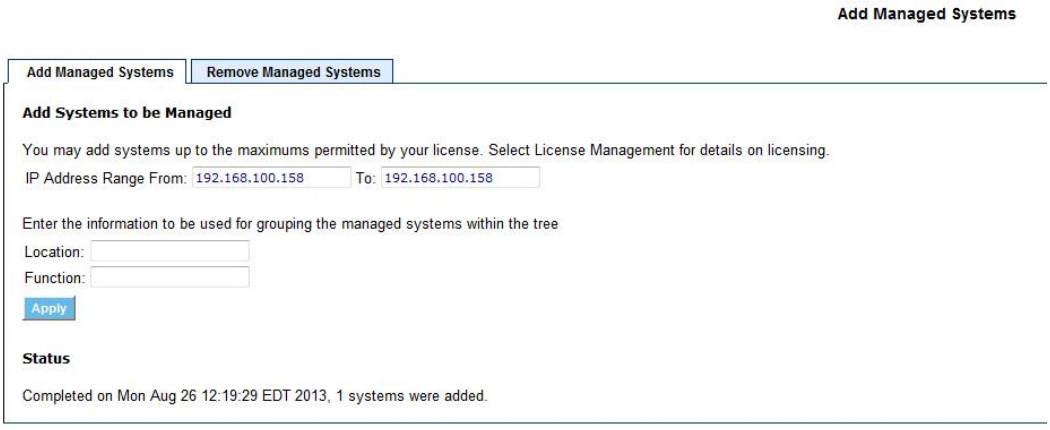
Once a system is added it will automatically unlock the System Client software running on that system, which will now send event messages to the System Area Manager software.

To add a system or discover systems to be added to the System Area Manager, choose Add Managed Systems from the drop down menu on the header bar.

1. Enter the IP addresses in the **From** and **To** fields. To add a single system, enter the same IP address in the **From** and **To** fields. To discover systems across a network address range, enter the lower IP address in the **From** field and the higher IP address in the **To** field.

   *It is recommended to keep the IP address range "dense". The longest wait times occur when trying to sample IP addresses that are not in use.*

2. Enter the **Location** and **Function** that is to be applied to the discovered systems. (These values are used in grouping and sorting of the tree.)
3. Click the **Apply** button.
4. You will now see a status of the addition scan saying how many systems have been scanned out of the total to be scanned.
5. You can cancel the scanning by pressing the **Cancel** button.
6. Once discovery has been completed the **Status** will show the number of systems successfully added.



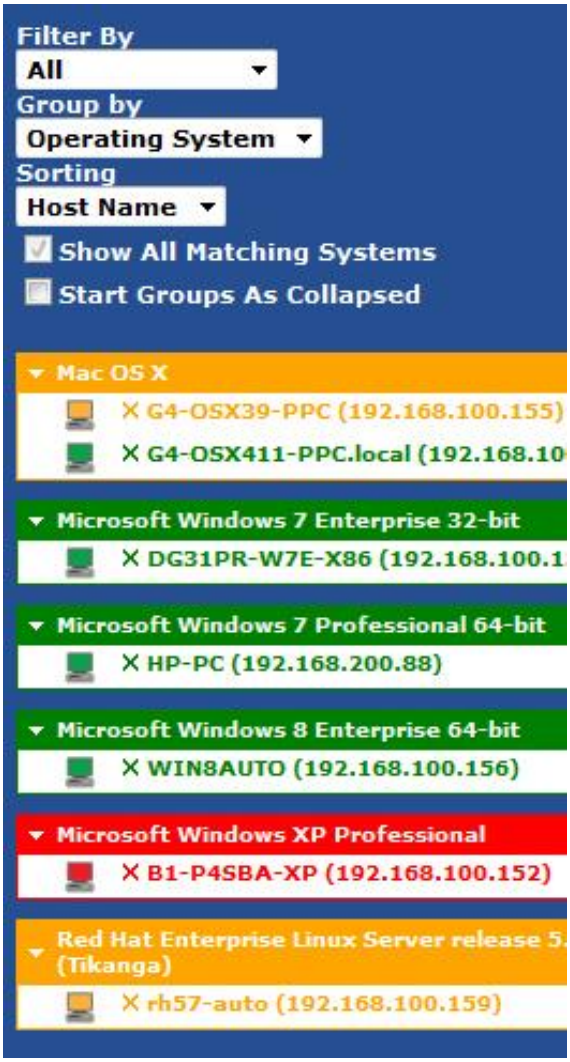

## Changing to which System Area Manager the system reports

Remove the system from the first System Area Manager tree to stop the system from reporting. Once this is done, add the system to the second System Area Manager tree by following the instructions "Add Managed System"

## Removing Managed Systems

If you wish to remove a single managed system from the System Area Manager Tree:

- Click on the <X> next to the name of the system
- You will be prompted to confirm the deletion of this system




If you wish to remove a group of systems choose the Add Managed Systems option from the drop down menu, then click the Remove Managed Systems tab.
Here you can choose to remove systems by an IP Address range, Function, or Location. You can also remove inactive systems based on how long they've been inactive.

If you choose to remove by IP Address Range, enter starting and ending IP addresses. All systems running the System Client within that range will be removed from being managed by the System Area Manager.

If you choose to remove by Function then you must choose one of your predefined functions. All systems running the System Client within the chosen Function will be removed from being managed by the System Area Manager

If you choose to remove by Location then you must choose one of your predefined locations. All systems running the System Client within the chosen Location will be removed from being managed by the System Area Manager

If you choose to remove by Date then you must choose the number of days the System Client has been inactive for. All systems running the System Client that have been inactive and not reported to the System Area Manager within the chosen option of 30, 60 or 90 days will be removed from being managed by the System Area Manager

When the removal process has completed, the number of systems that were successfully removed from the System Area Manager will be displayed.

*Once a system has been removed from the Management Tree the System Client software will go back to email alerting only and will not report its events to the System Area Manager.*

The system you removed is still being monitored for health by the management agent on that system, which will alert via email to any issues it discovers. You may add the system back into the System Area Manager tree at any time.
If you wish to completely disable this monitoring on the removed system, uninstall the software on that system.

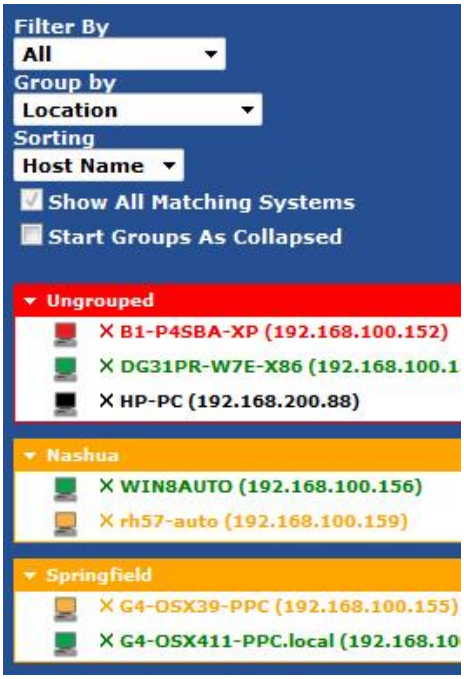
# Filter by, Grouping and Sorting Options for the Management Tree

Systems listed on the Management Tree are filtered by showing all health states and grouped by operating system and sorted by machine name by default. By using the Filter By drop down menu, administrators can choose to only show a certain health state, helping the administrator to narrow down their view to only systems with a certain health state.

By using the Group By drop down menu, administrators can choose to view groups of systems by location or by function, helping the administrator to narrow down issues in environments with large numbers of systems.

By using the Sorting drop down menu, administrators can select to view the systems within the groups by Machine Name or IP Address within the groups; this reverses the display order to IP Address/Machine name for IP sorting order and Machine Name/IP Address for Machine Name sorting order.

The administrator can modify the **Location** and **Function** fields in the System screen for each managed system. If this information has not been specified for some managed systems, the grouping function will display the systems as “Ungrouped” as the name for the location or function.



If Server, Desktops and Notebooks are being monitored the Subgroup option will be displayed.

By clicking on the Subgroup check box, the tree will be shown where the sorting within the chosen group will show the all Servers first, then Desktops and then Notebooks.

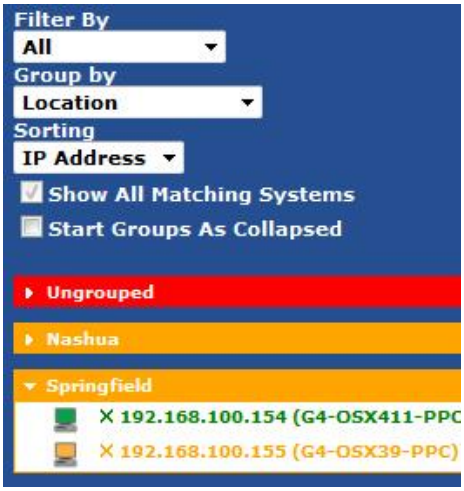
If Subgroup is not chosen then the sorting will be in the chosen order without any sub grouping of server/desktop/notebook.

The administrator can use the Filter By to choose to only show systems at a specific Health State.

## Expanding the System Area Manager Tree

System Area Manager provides administrators with an overall view of managed systems, and the capability to drill down to each system and individual components.

Click on the name of the operating system, function, or location to expand the list of systems in each group. The names and IP addresses of each system will be displayed in the left hand window.



## Tree Icons

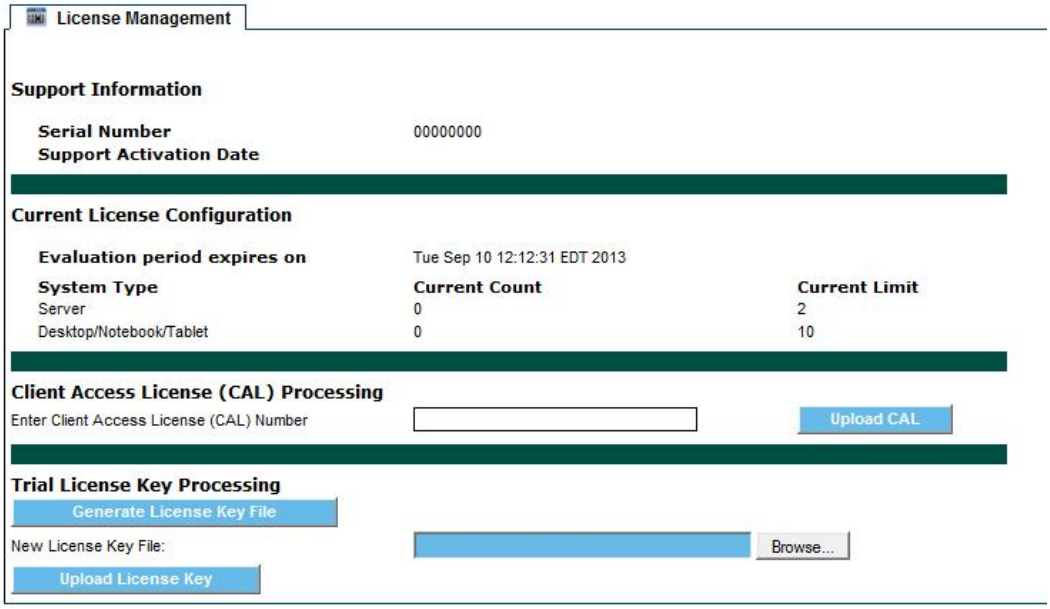
| | |
|---|---|
| | System Alert Matrix – Provides access to the thresholds, sample and reset periods, and notification options for all of the monitored hardware and software sensors within the system |
| | Remote Management – Provides access to the remote functions, Shutdown, Restart, Wake on LAN and Remote Console which provides the administrator full access to the remote systems keyboard, mouse and screen.<br>IPMI – Provides access to IPMI Event log data while system is running, also provides IPMI Over LAN Power Management and Event Log access out of band (system may be powered off). |
| | System – Provides system board, memory, CPU, slot, display, port information and status of the CPU and Memory utilization being monitored, in addition memory error information is displayed. |
| | Hardware – Provides sensor information and current status on physical sensors being monitored within the system. |
| | Network – Provides network adapter configuration information and performance for all configured adapters within the system. |
| | Storage – Provides physical storage device, storage controller, logical device information and health status for the storage devices and managed RAID controllers. |
| | Software – Provides information on OS services, processes, and installed applications. Also provides remote and process management. |

# Chapter 4: License Management

System Area Manager provides the ability to manage up to 2000 systems from a single user interface. The number of systems that can be managed is controlled through a Client Access License (CAL).

The software ships with a 15 day evaluation license that enables full System Area Manager capabilities to a limited number of systems.

Note: If the evaluation period expires, you will no longer be able to manage systems, but you will still be able to access the License Management screen and enter the Client Access License number.

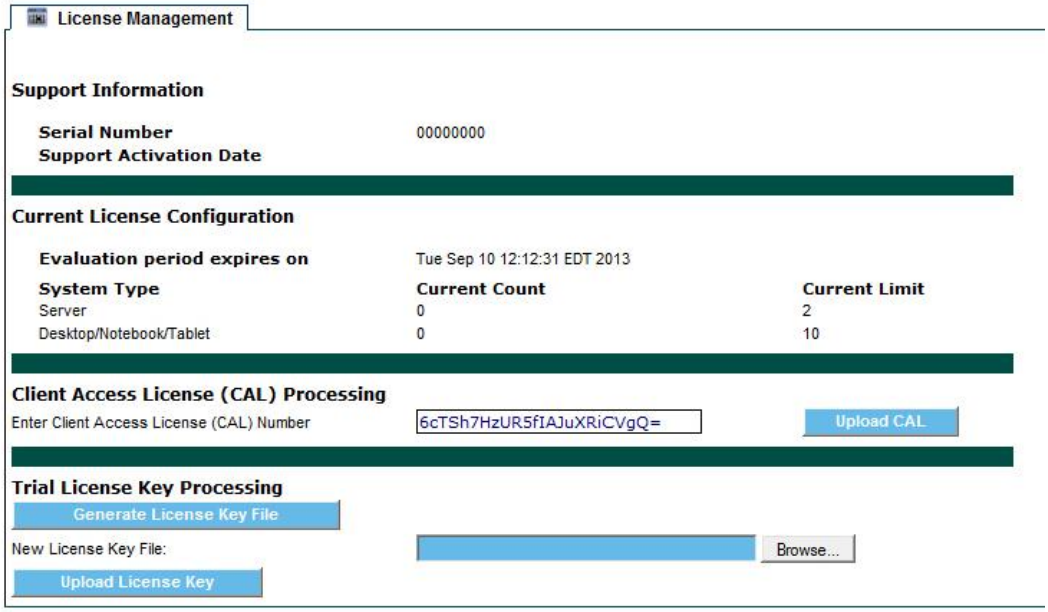



To unlock the ability to manage more systems, or for continued use after the evaluation period has expired, a Client Access License must be purchased.

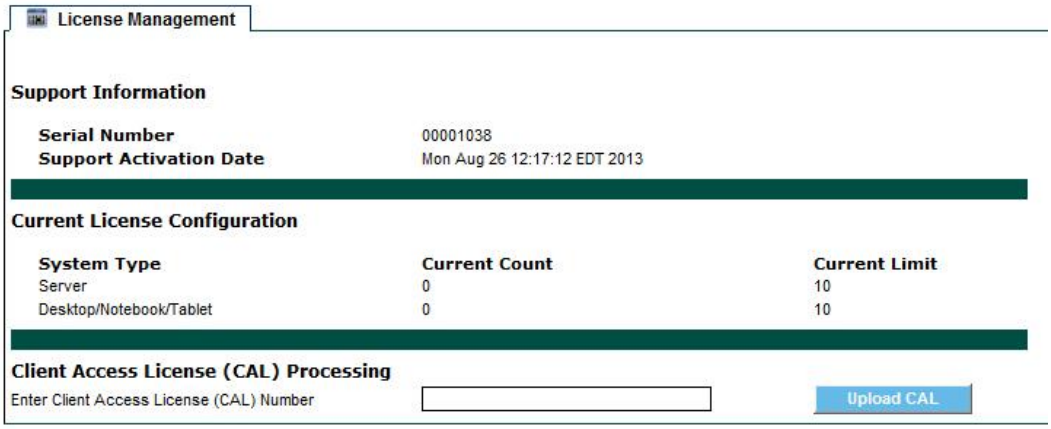
To access the License Management screen, choose it from the drop down menu on the header bar.

1. Open up the License Management screen on the System Area Manager that you wish to enter the Client Access License for.
2. Enter the Client Access License number into the box and press Upload CAL.
3. The System Area Manager will process the Client Access License and the current limits will be increased to the limits that you purchased.
4. If this is the first time you purchased a key for this System Area Manager you will be provided with a support Serial Number and when Support Activation Date.

The CAL can be manually entered or pasted into the entry box.




Once the CAL has been entered the software will be issued a serial number and Activation Date.



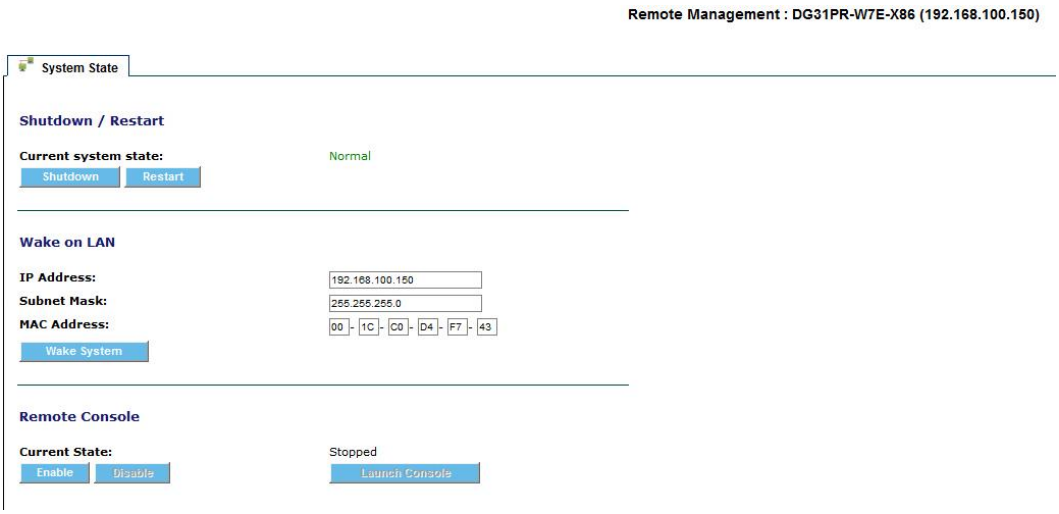
# Chapter 5: Remote Management

System Area Manager provides remote management functions for its managed systems, including Wake on LAN, Shutdown, Restart, Remote Console and for AMT enabled system it provides, AMT power Management, for IPMI enabled systems it provides IPMI Event Log and IPMI Over LAN for IPMI.

To access remote management, choose this option from the listed system on the System Area Manager tree.

## System State

The system state screen contains information on the current condition of the selected system, using the same health color scheme. System Area Manager remote management provides Shutdown / Restart, Wake on LAN and Remote Console management options. In order to use the Shutdown, Restart, and Remote Console management options, the System Client software must be running.




To shut down or restart the system, the system must be in Normal, Warning or Critical health states.

- To shut down a system, click Shutdown.
- You will be prompted to confirm this action.
- To restart a system, click Restart.
- You will be prompted to confirm this action.

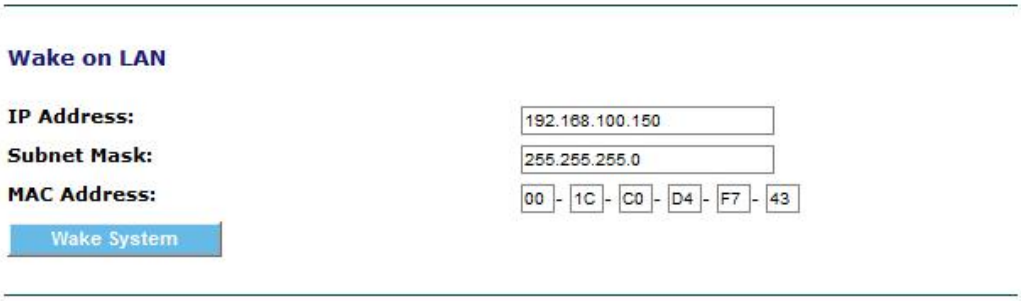
# Wake on LAN

Wake on LAN capability allows central administrators to power up a WOL enabled managed system. In order for Wake on LAN to function properly, the administrator must have enabled this capability within the managed system's BIOS.

To wake a system, the system must be in the Shutdown health state.

- The IP address and MAC address of the system is automatically populated by the System Area Manager.
- Click the Wake System button to wake the system remotely.

The administrator can change the MAC Address and IP Address of the network connection to be notified with the WOL command. Use this when the managed system is reporting to the System Area Manager on the non WOL-enabled network adapter. Note that System Area Manager will need to be able to access the WOL enabled Network adapter for this function to work.




# Remote Console

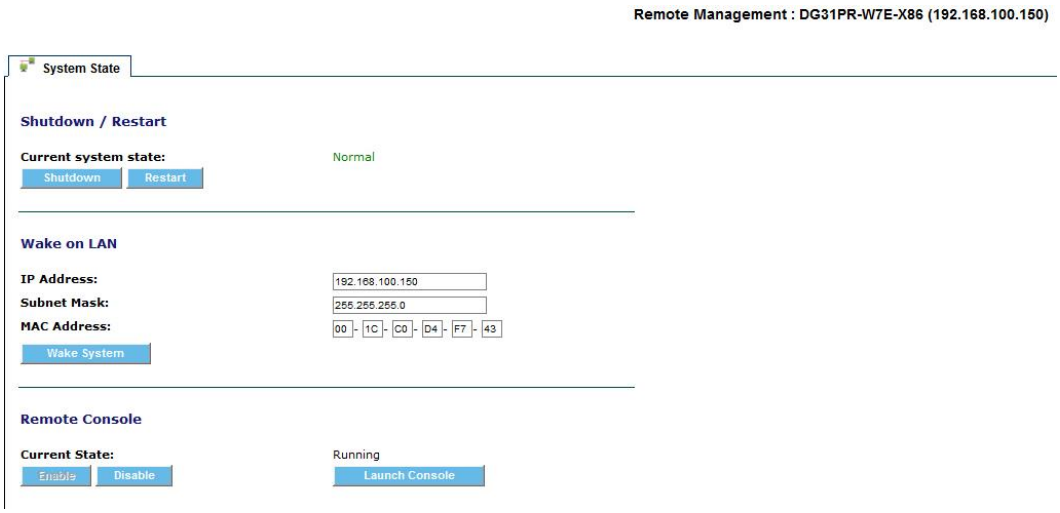
Remote Console provides the capability of taking control of a managed system’s local screen, keyboard and mouse directly through the Server/Desktop System Client interface.

To access the Remote Console, select the system from the Management Tree, then click the Remote Management icon, to open the remote management screen. The bottom section of the screen shows the Remote Console status and Enable/Disable and Launch Console buttons.

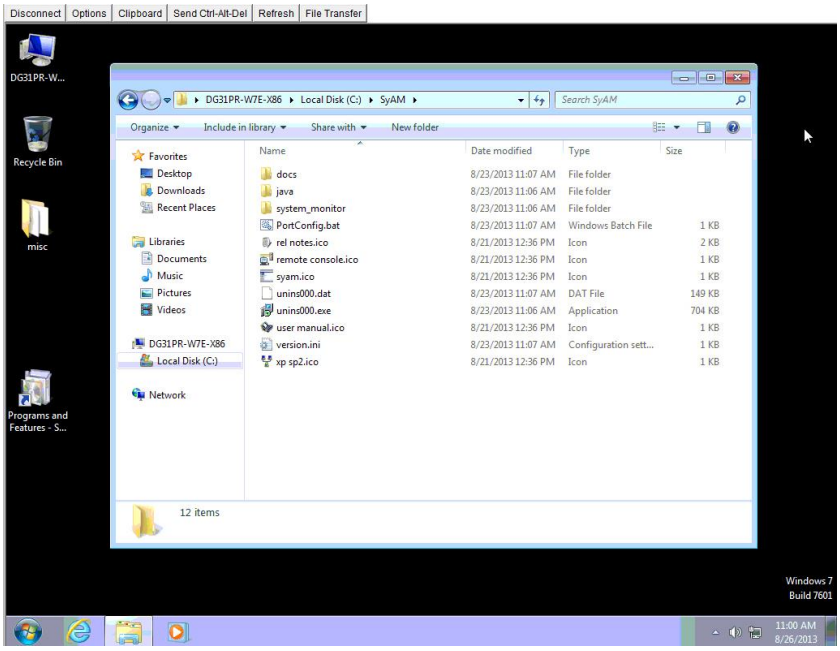
The status must be Running if you wish to launch the console.

Click on the Enable button to start the service on the remote managed system.
Click on the Disable button to stop the service on the remote managed system.
Click on the Launch Console button to establish a remote console session.

We recommend you disable the remote console feature (which stops the software from running) after each use; however the software will automatically be stopped once the managed system is rebooted.

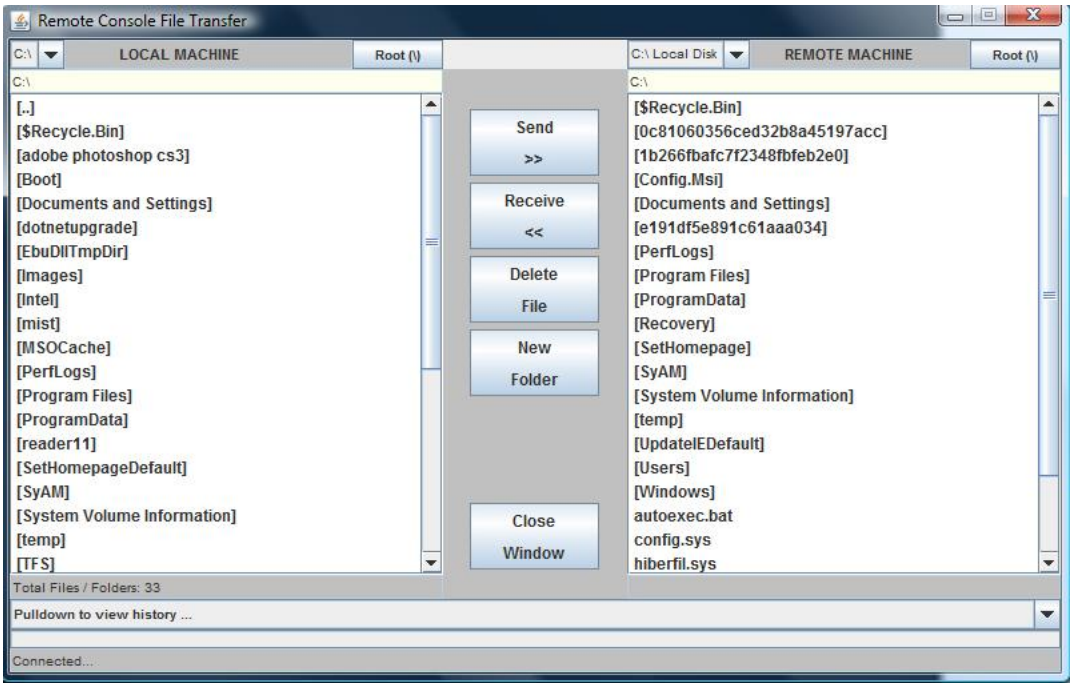



Once you have launched the remote console, enter the password (the default for Windows is 1234) and the console session now provides access to the remote system.




When finished, click Disconnect to close the window.

For Windows systems the Remote Console function offers a File Transfer option. To transfer files to and from the system you are accessing via Remote Console, click the File Transfer button at the top. This will open a Remote Console File Transfer window.




Navigate to the file on the Local Machine or the Remote Machine and click the Send or Receive button.

Receive will transfer the file from the Remote Machine to the machine you are browsing from.

Send will transfer the file from the machine you are browsing from to the Remote Machine.

.

## Changing the Default Password

On Windows:

Please use the Management Utility software version 4.30 or above

On Linux:  Default password is 12345678

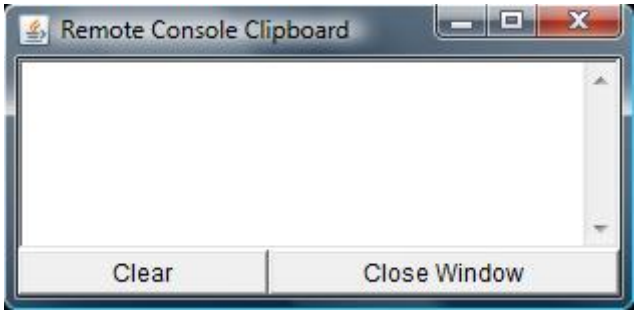
cd to the top-level directory where the System Area Manager software was installed.  From there:

```
cd system_monitor/remote_console
./vncpassword
```

You will be prompted to enter and then confirm the new password.

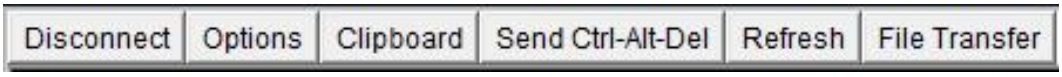
## Using the Clipboard

To copy information from the managed system to the local System Area Manager, select the information to copy and use the edit/copy command, then click on the Clipboard button at the top menu, then paste the information to the clipboard.  Now select the information in the clipboard and copy/paste it into a file on the local system.




## Ending the Remote Console Session

To end the Remote Console session, click the Disconnect button in the top menu.



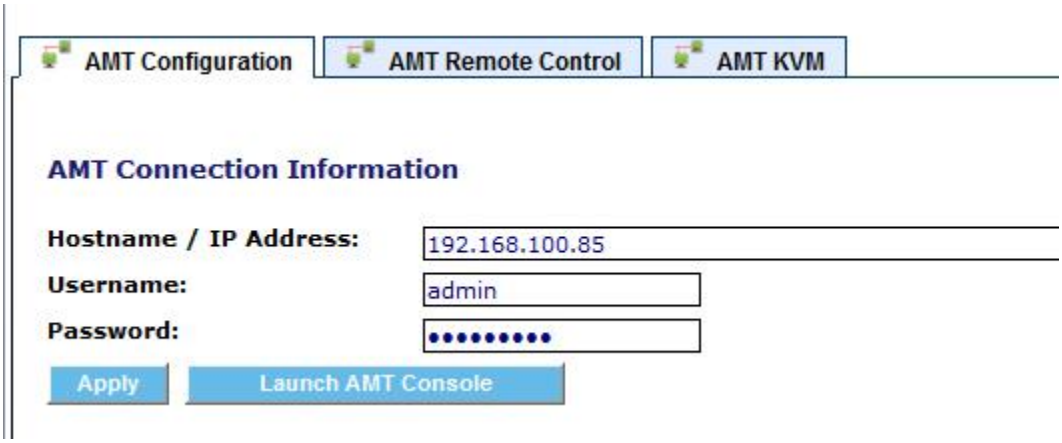
# AMT (Intel® Active Management Technology)

The AMT Tab will only appear if the system running the System Client is identified as having Intel AMT technology onboard.

Server/Desktop/Notebook System Client can provide power management and AMT Console access when the system is in either an operating system-present or -absent state.

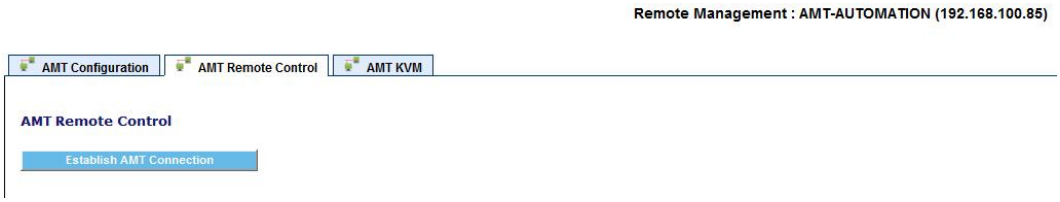
*Please check* [www.syamsoftware.com/vpro](http://www.syamsoftware.com/vpro) *for validated AMT configurations.*

You must first configure the AMT Port IP address and password using the vendor provided utilities before you can utilize this AMT feature. Enter the user name, password and IP address of the AMT port for the managed system. Click the Apply button to save this data.




Click Launch AMT Console to open a new browser window and login directly into the embedded AMT web server.

Once you have saved the user name, password and IP address, click the Establish AMT Connection button under the AMT Remote Control Tab to access the managed system's AMT over the LAN.




Once connected, the following power options are available.

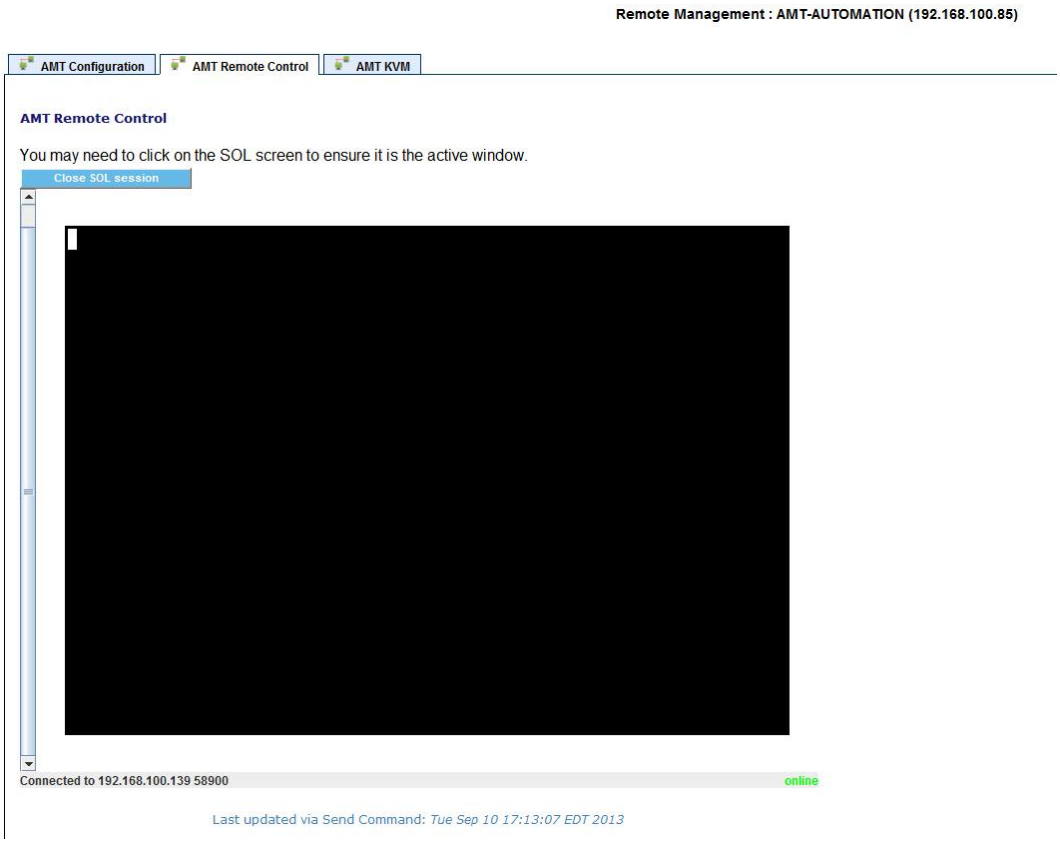
**Power Off**
This will perform a forced power off not a graceful shutdown.
**Power On**
This will perform a forced power on.
**Power Reset**
This will perform a power reset not a graceful reset.
**Power Cycle Reset**
This will perform a power cycle reset.

Serial Over LAN enables a user to remotely reboot a system. When a user reboots with SOL enabled, the SOL session is presented in the user's browser.

In order to create an SOL session, the user must verify the current power status.

Next, click the 'Launch SOL Session' box, and then click on the 'Send Command Button'.

***Please Note:*** *When using an SOL session, you are only able to boot the system normally. You cannot specify special commands such as PXE.*

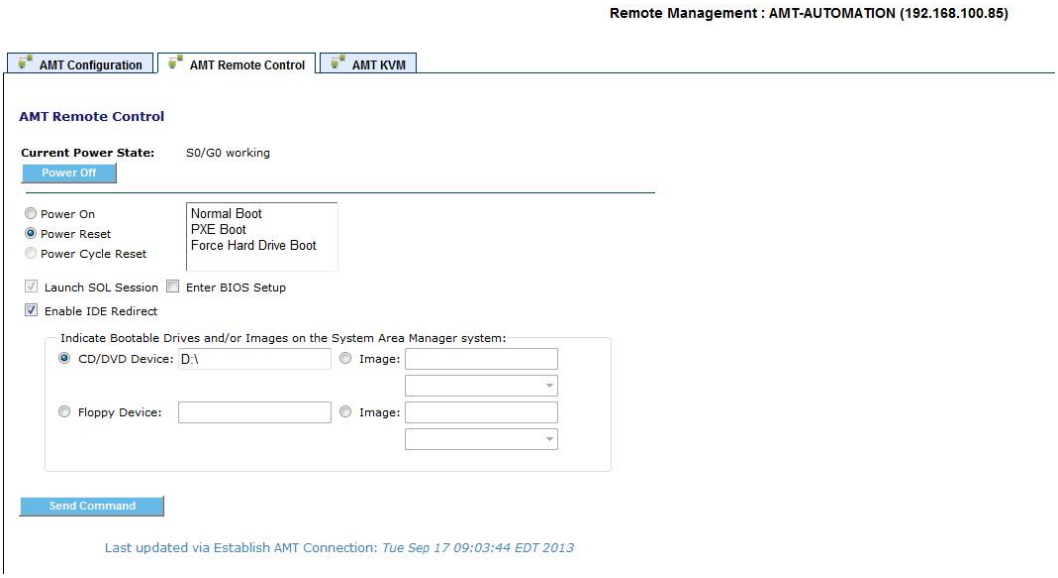



IDE-Redirect allows an AMT managed system on the System Area Manager tree to boot from a CD/DVD Image, floppy image, floppy disk, CD or DVD device which is located in the system running System Area Manager. IDE-Redirect is only available when using SOL.

These drives or images are on the computer running System Area Manager, NOT on the computer running your web browser. The default folder for storing these images is:

C:\SyAM\IDER\

To invoke the IDE Redirect either click on the Power Reset or Power On buttons and click in the SOL and IDE-R check boxes. Under image chose one of the four options, Floppy Image, Floppy Drive, CD/DVD Image or CD/DVD Drive you want the system to boot from, and click ‘Send Command’.




When using either a Windows or Linux System Area Manager you need to use the correct corresponding Windows or Linux syntax for the Floppy disk device and CD ROM device.

If you are unsure of what the logical letter of the CD ROM device is, browse to the Storage screen of the System Area Manager.

System Area Manager running on a Windows Operating System

Floppy Device Drive **a:**
Floppy Device Image **c:\win98dos.img** or **c:\win98doscd.iso**

CD Rom Device Drive **d:**
CD Rom Device Image **c:\win98doscd.iso**

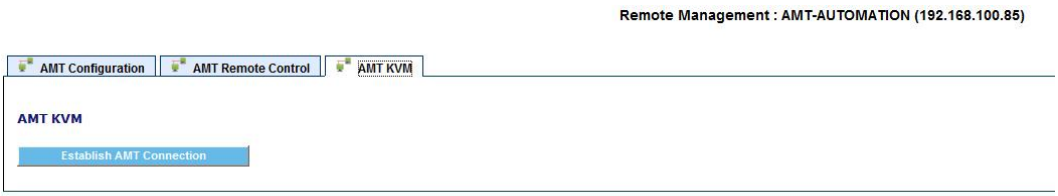
System Area Manager running on a Linux Operating System

Floppy Device Drive **/dev/fd0**

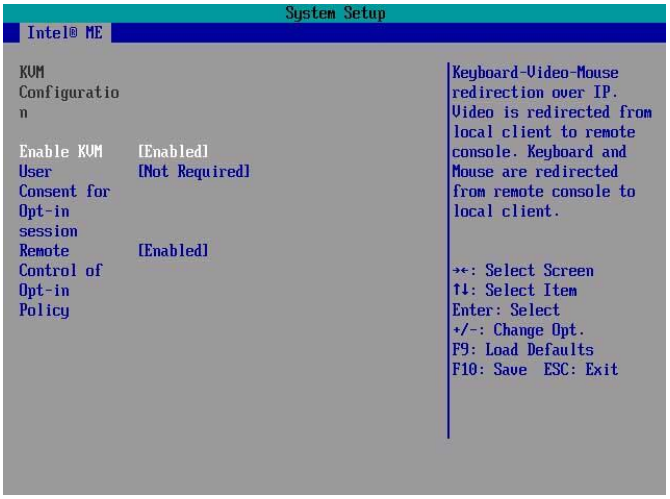
CD Rom Device Drive **/dev/hda**

## AMT KVM

If you have an AMT 6 or above capable system you will be presented with a 4th AMT Tab called AMT KVM.




**Note:** Your Management Engine (ME) must be configured to support KVM. This requires a processor with integrated graphics such as an i5 Processor. Please check your hardware manual for the list of supported processors for the KVM capability.



When you click on the Establish AMT Connection you will open up the AMT KVM configuration screen. If your system does not have the AMT KVM configured in the ME you will be presented with an error message, **"KVM must be enabled in your management engine".** Please recheck your ME settings and make sure the KVM is enabled.

By checking off the Local User Approval Required you will require the user to provide you with the pass-code presented on their screen and enter this onto your interface before you can take remote control of their system. The timeout is the number of seconds you have to enter this code before the remote connection is closed.

The KVM Password is the password programmed into the ME, this is required to log into the Remote system's KVM. The password must be 8 characters and contain upper and lower case, numbers and characters. Example: P@ssw0rd

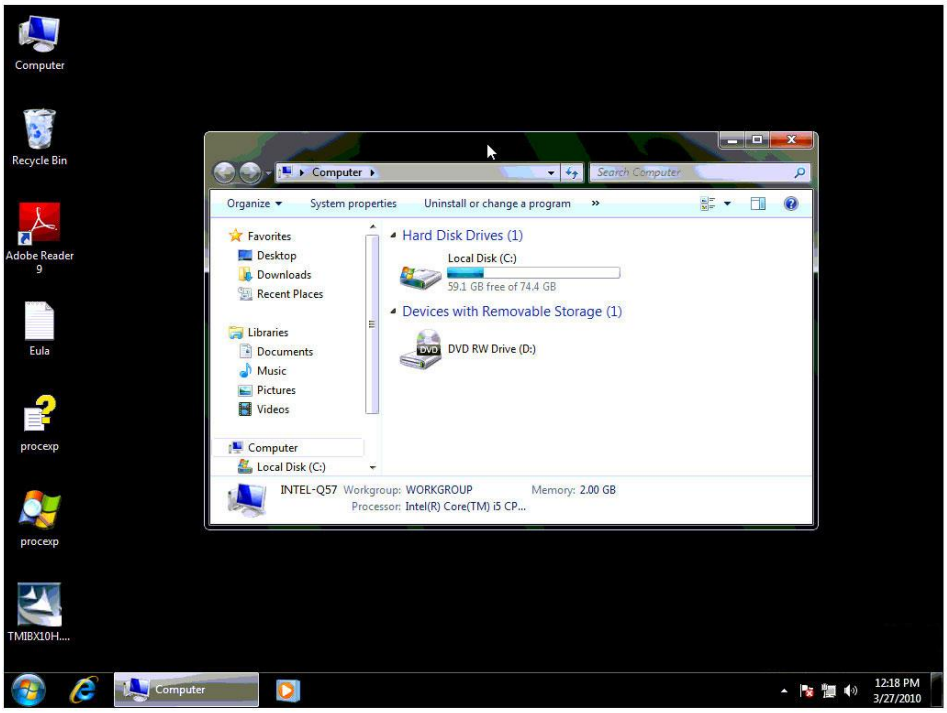
The KVM Inactivity Timeout is the number of minutes the remote KVM connection will disconnect with the remote system when there has been no mouse or keyboard activity to the remote system through the browser.

After you have applied the password and settings you must start the KVM before you can launch the KVM. You can stop the KVM after it has been used for additional security.

When you click the Launch KVM button you will be presented with the KVM Authentication screen.

Enter the Password that you configured in the KVM screen.

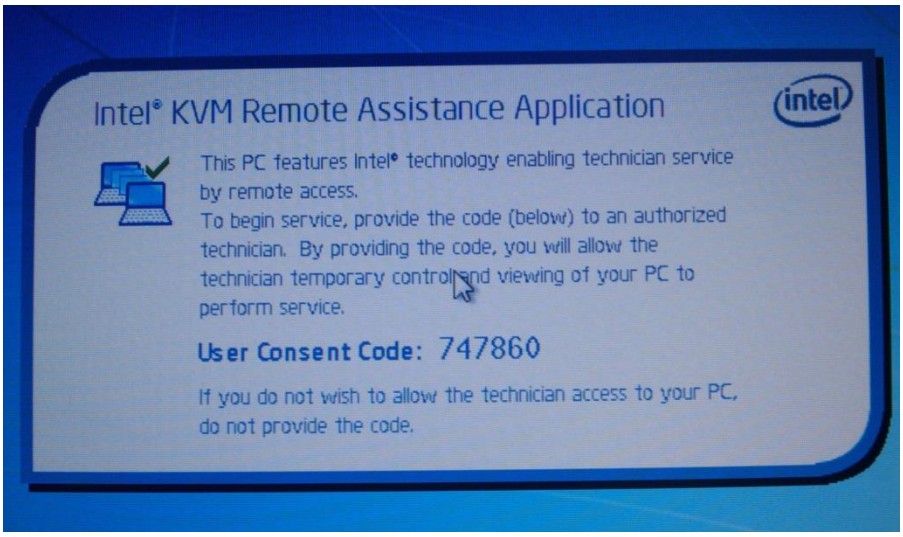
If you have not enabled the Local User Approval you will now be presented the KVM of the remote system.

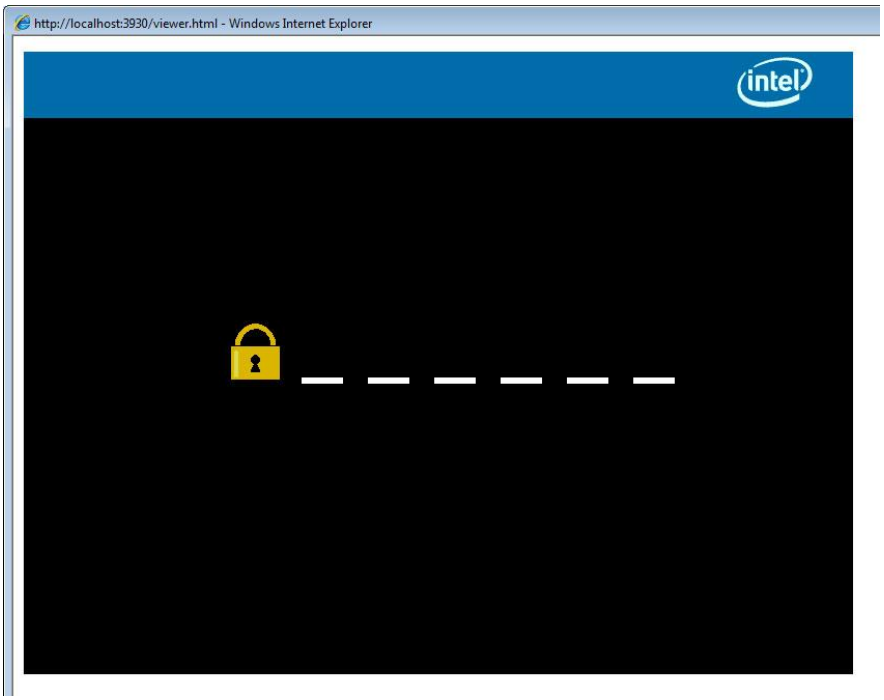



Close the window when finished.

**Please Note**: If you have AMT KVM running you will not be able to use the Remote Console feature in System Area Manager.

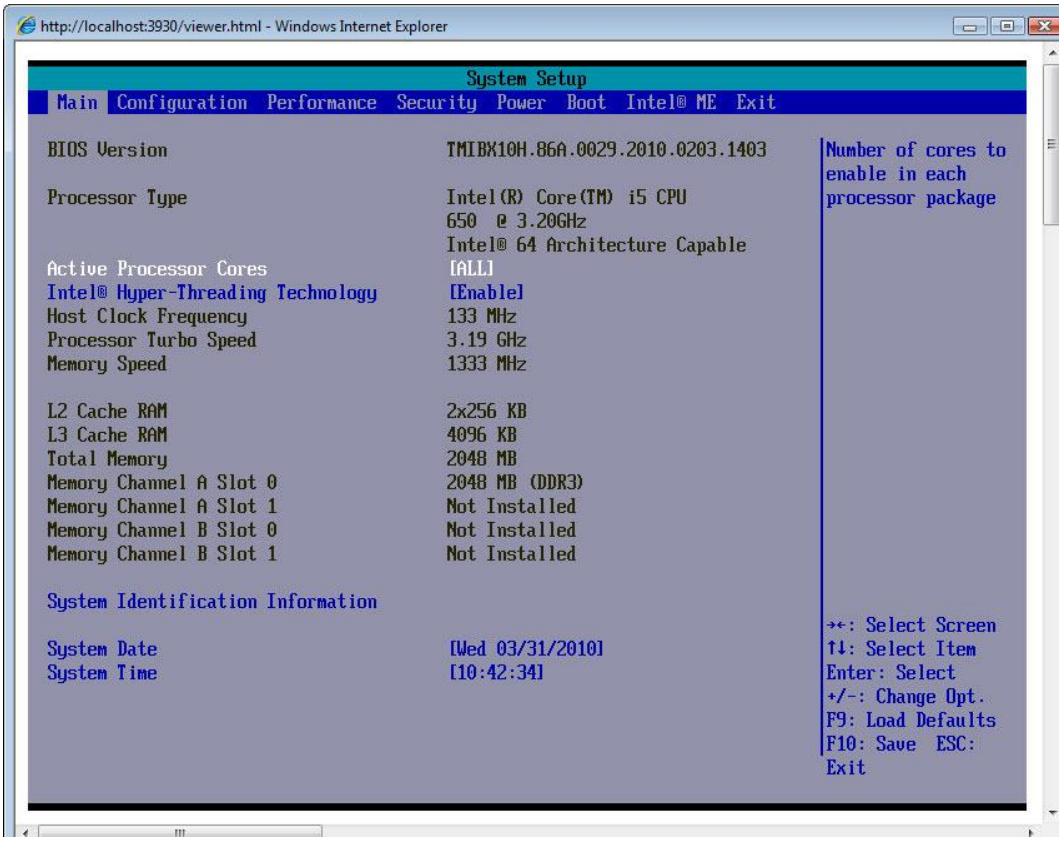
If Local User Approval is enabled have the end user provide you the pass code on their screen and enter it onto your screen so you can take KVM control of their system.




Once you enter the code the KVM will be connected to the remote system.

The KVM works even when the system is powering up so you can make BIOS changes, to do this on your System Area Manager choose restart the system from the Remote Management page or choose to Power Reset or Power On for the system from the AMT Remote Control page, then press F2 on the KVM window to enter setup.



# IPMI Event Log

Server System Client can monitor physical events occurring on IPMI-enabled servers that are being managed. These events are recorded in the IPMI Event Log, which is accessible through System Area Manager. Each event is given a unique number and dated. This information, as well as a description of the event type, sensor type affected, and event alert type are recorded in the IPMI Event Log.

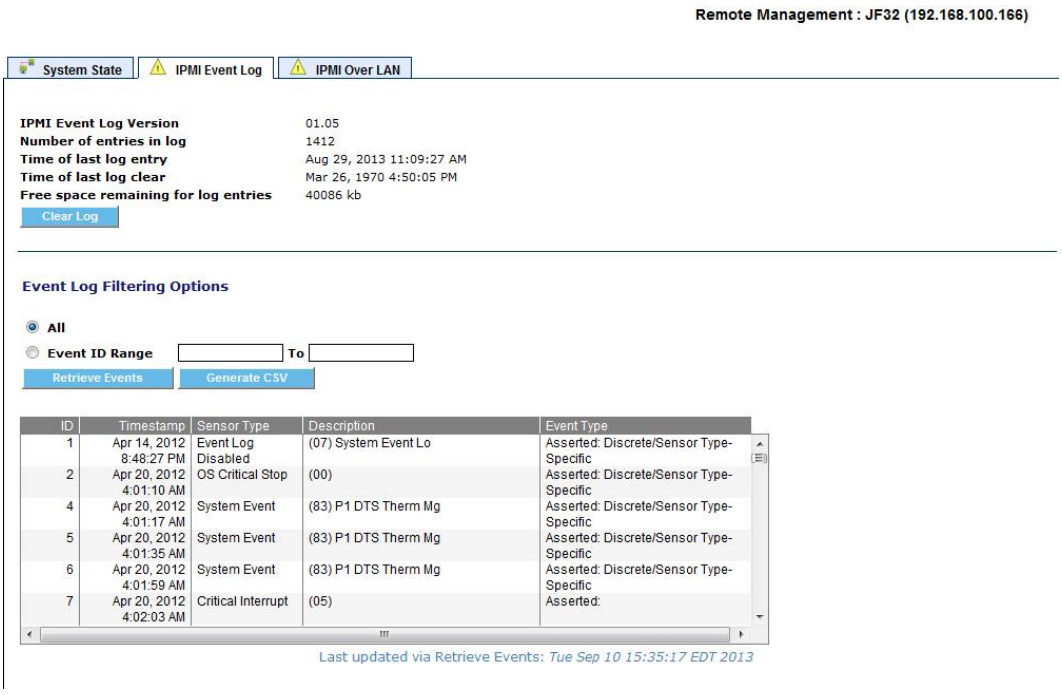
In addition, the IPMI event log lists the version of the log, the number of entries in the log, the last time an entry was added, the last time the log was cleared, and the free space remaining for the log.

The log can be reviewed and filtered by listing all events, or by filtering by an event range. The results can be displayed on the screen or exported to a file in .CSV format without clearing the log.

The IPMI Event Log allows administrators to retrieve and view all events occurring and reported by a specific server. In order to access the IPMI Event Log, the system must be IPMI-enabled and running a valid version of Server System Client.

Fields included in this screen are:

- IPMI Version
- Number of entries in the log
- Last time an entry was made in the log
- Time of last log clear
- Free space




The IPMI Event Log provides administrators with the option to clear or purge the log, by clicking the Clear Log button. Note: this action cannot be undone.

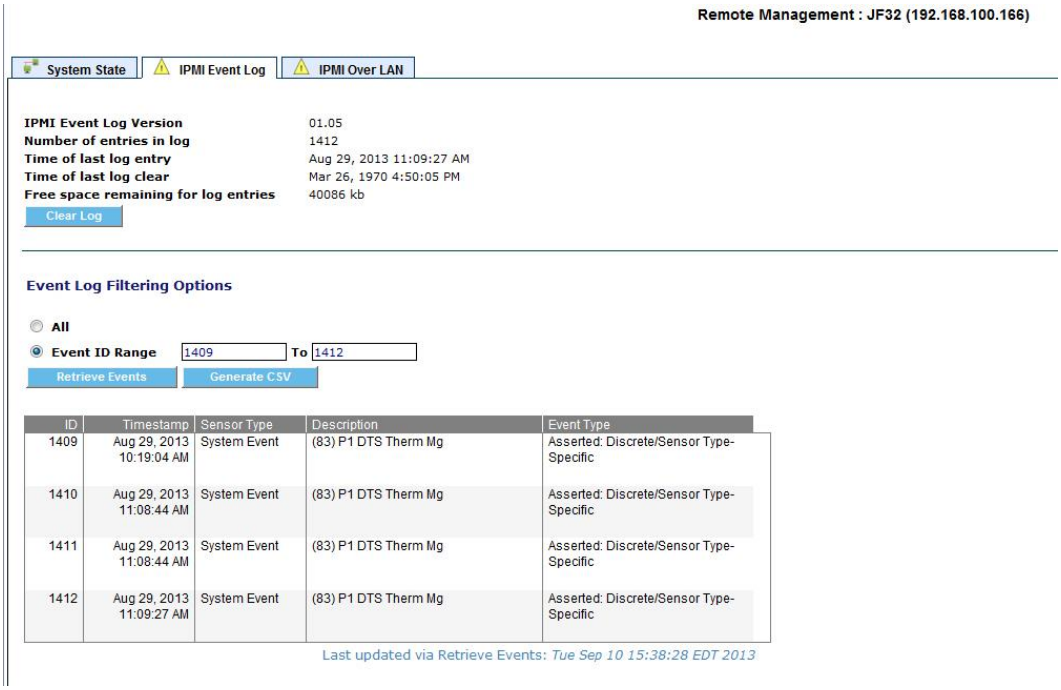
## IPMI Event Retrieval

The IPMI Event Log provides administrators with the option of retrieving and viewing some or all events recorded for the server, and sorting them by type.

To retrieve all of the events from the IPMI event log stored on the BMC, click the radio button next to "All".

To retrieve a subset of events, enter a beginning and ending Event ID. The beginning Event ID value must be either 0 (to retrieve from the beginning of the log), or an actual Event ID number. You will receive an error message if a non-0 Event ID cannot be found.

Then click on the Retrieve button. The results will be displayed in the detail window at the bottom of the screen.




The ID values assigned to events are generated by the IPMI controller, and are dependent on how the system's firmware has been configured. As a result, the Event ID may differ by server platform.

**Generate CSV**

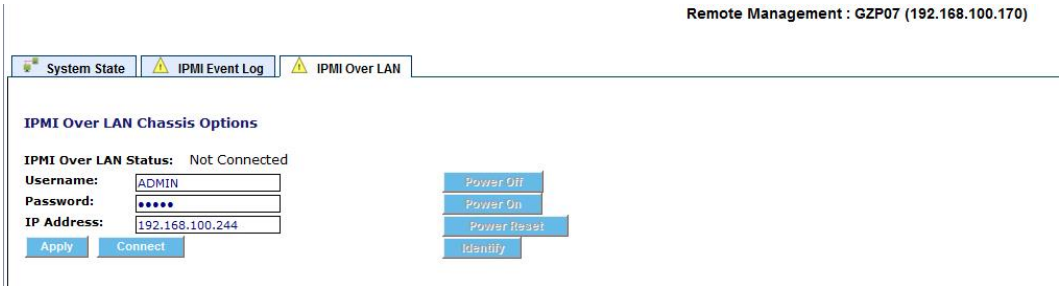
This button retrieves the events and saves them to a CSV file.

# IPMI Over LAN

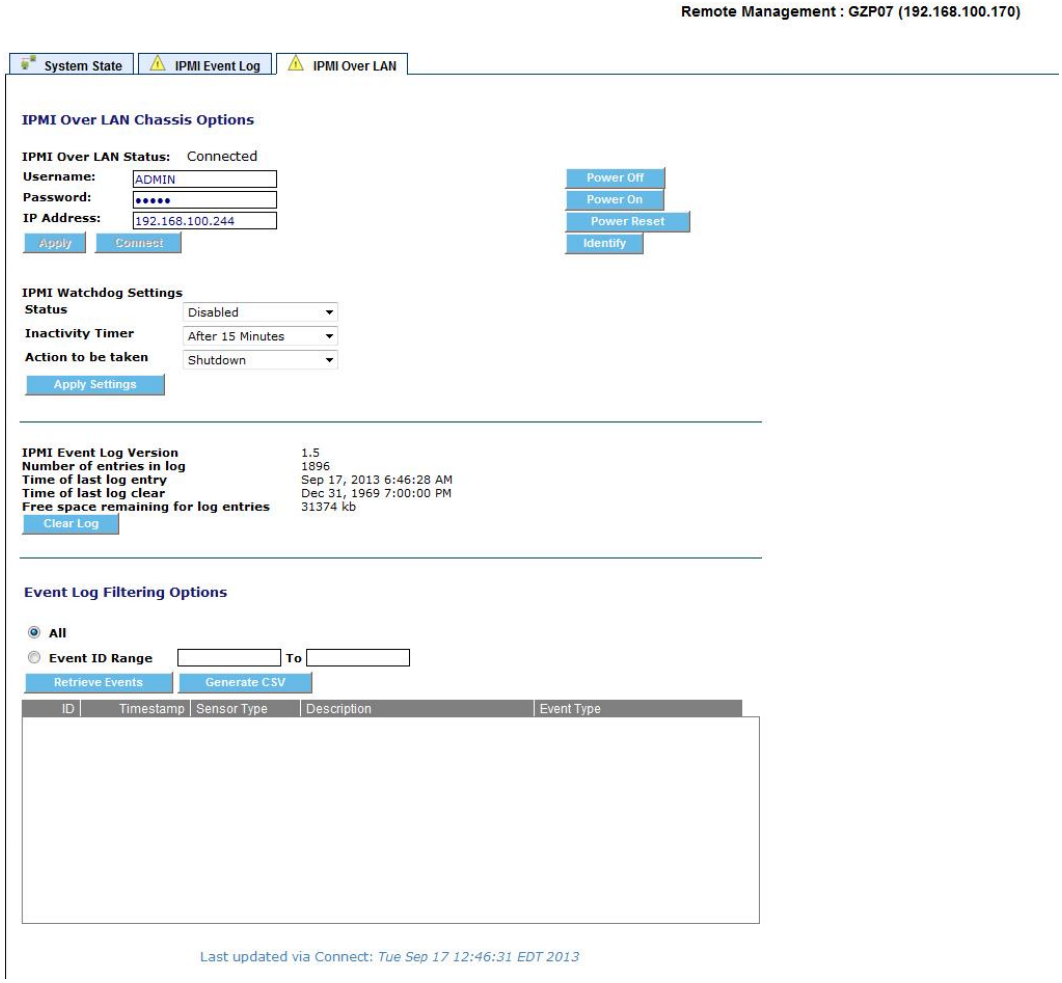
Server System Client can provide IPMI Over LAN power management and event log capabilities when the system is in either an operating-system-present or -absent state.

You must first configure the BMC's IP address and Password using the vendor provided utilities before you can utilize this IPMI Over LAN feature.

Enter the user name, password and IP address of the BMC for the managed system, then click on the apply button to save this data.




Once you have saved the user name, password and IP address, click the Connect button to access the managed system's BMC over the LAN.



Once connected, you can perform the following options.

**Power Off**
This will perform a forced power off not a graceful shutdown. **The operating system may or may not receive notification and shut down, this varies by hardware platform.**

**Power On**
This will perform a forced power on.

**Power Reset**
This will perform a power reset not a graceful reset. **The operating system may or may not receive notification and shut down, this varies by hardware platform.**

**Identify**
This will light the identification LED of the system. This feature is not supported in all hardware platforms.

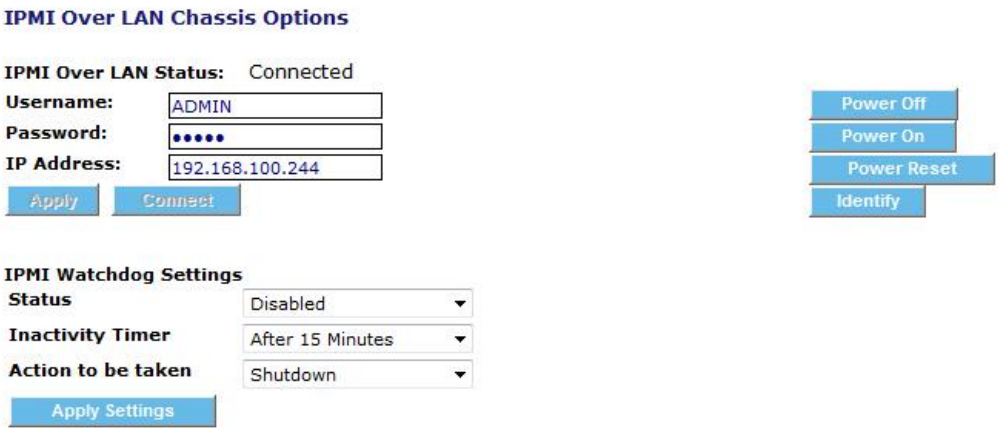
**Event Log**
The IPMI Event Log is accessed in exactly the same manner described above.

## IPMI Watchdog

IPMI Watchdog is a feature that allows the BMC to shutdown or reboot the server when the operating system becomes unresponsive. When enabling this feature you define the number of minutes that the operating system can stop responding before taking the action of shutdown or restart.

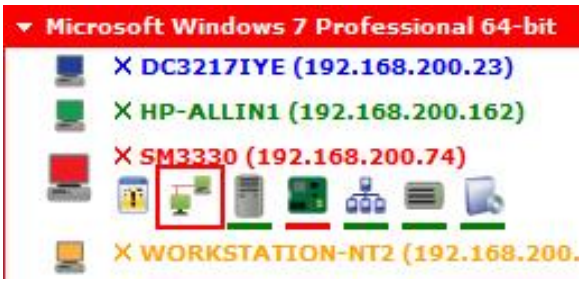
The IPMI Watchdog Settings will only be displayed and configurable if the System Client is functioning.

***This feature is disabled if the System Client is un-installed or the System Client service is stopped.***



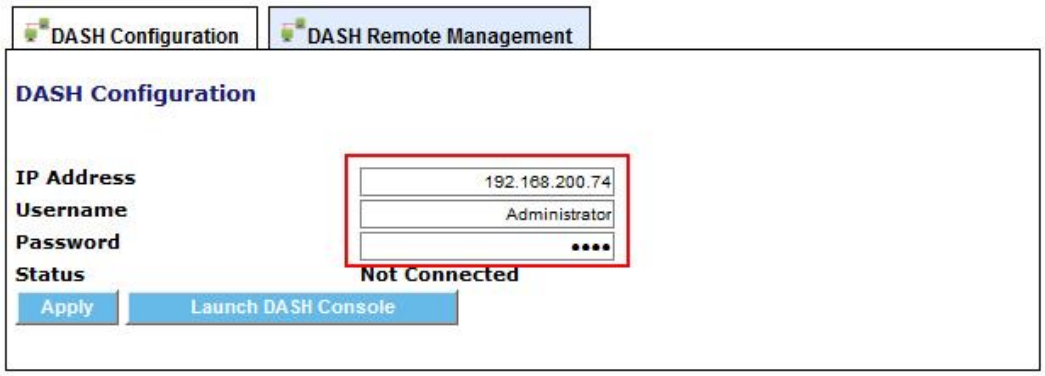
# DASH (Desktop and Mobile Architecture for System Hardware)

The DASH standard allows secure remote and out-of-band systems management. The DASH tab will appear in the Remote Management interface if this feature is supported by the system hardware and System Client version.



Clicking the DASH tab displays the DASH Configuration and DASH Remote Management tabs. In DASH Configuration, enter the DASH out of band authentication information as configured for the client, and click Apply to save your configuration. The IP Address box is automatically populated with the IP address used by the operating system. Some systems will require a different IP address for the DASH connection. If the OS is configured to use DHCP, and DASH is configured to use the same IP address, do not edit the IP Address field as any change will cause it to be treated as a static IP address. The system name can be used instead of the IP address.

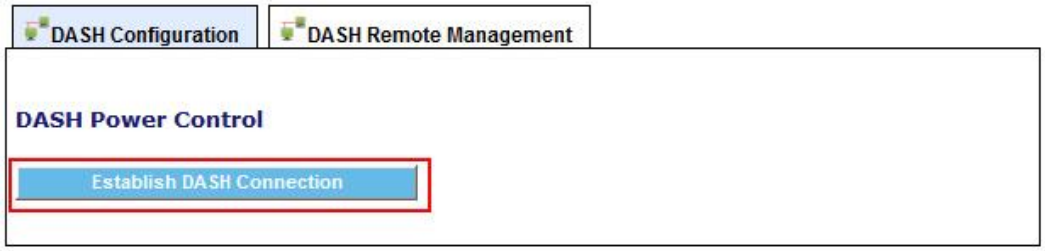
Click the Launch DASH Console button to open a new window and log in to the system's embedded DASH management console.



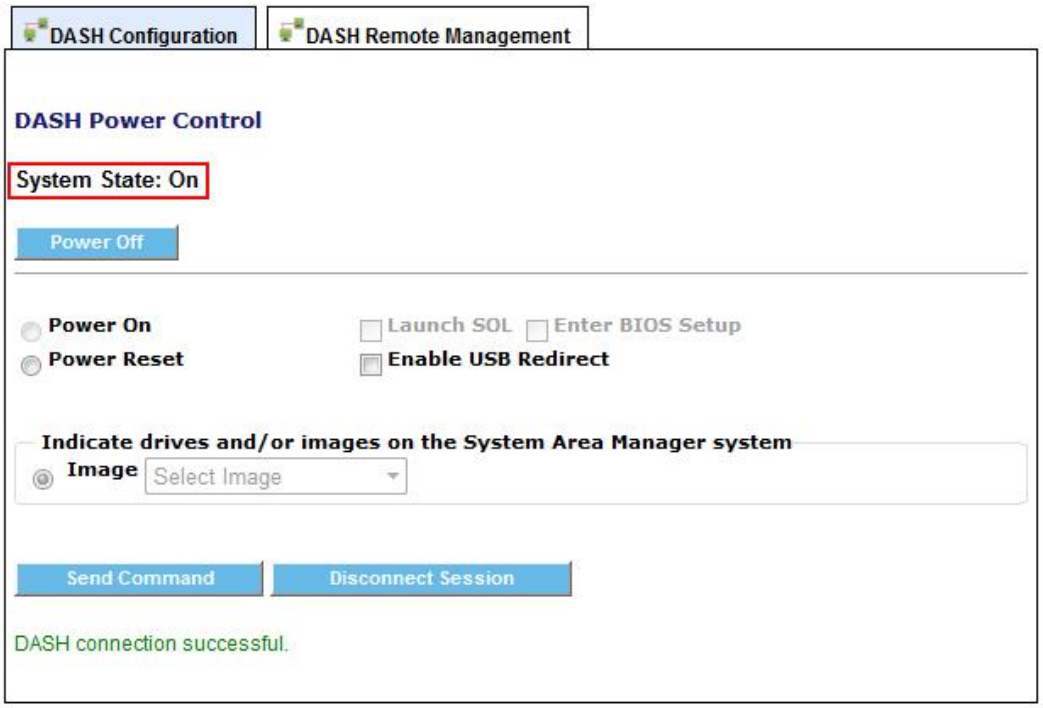

## DASH Remote Management

With DASH configured in System Area Manager, direct power control of supported systems is enabled.

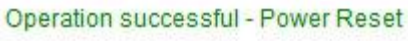
1. Click the DASH Remote Management tab, then click the Establish DASH Connection button.



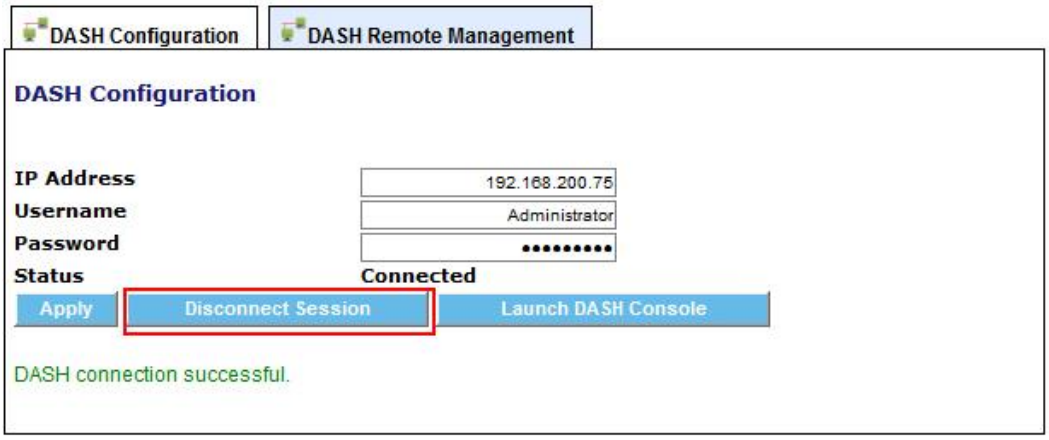

2. The current power state of the system will be displayed.



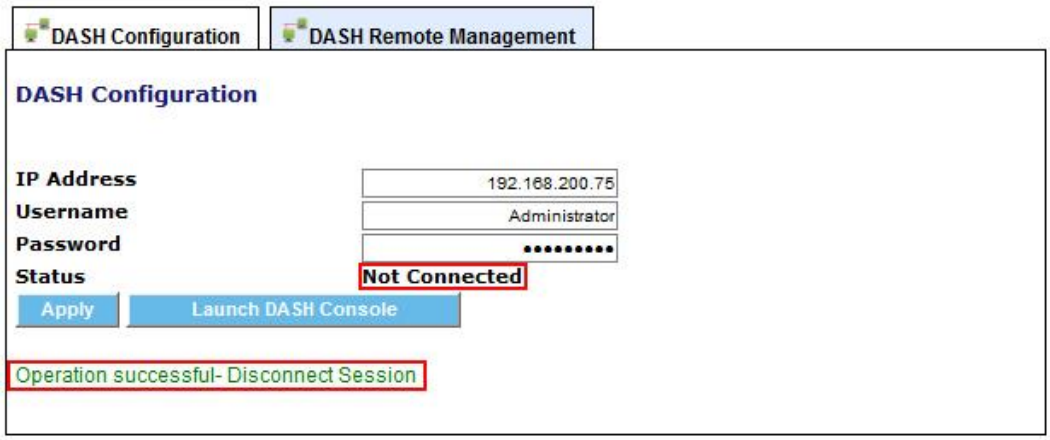

3. Choose a power option. If the system state is On, clicking the Power Off button will cause a shutdown. You can also click the Power On radio button (if the system state is Off) or the Power Reset button (if the system state is On), followed in either case by clicking the Send Command button. The result of the chosen power command will be displayed at the bottom of the screen.




4. **When finished, you must disconnect the DASH session by clicking the DASH Configuration tab, then clicking the Disconnect Session button. Remote sessions will be left connected if they are not disabled.**




5. Once disconnected, the system status will update to Not Connected.



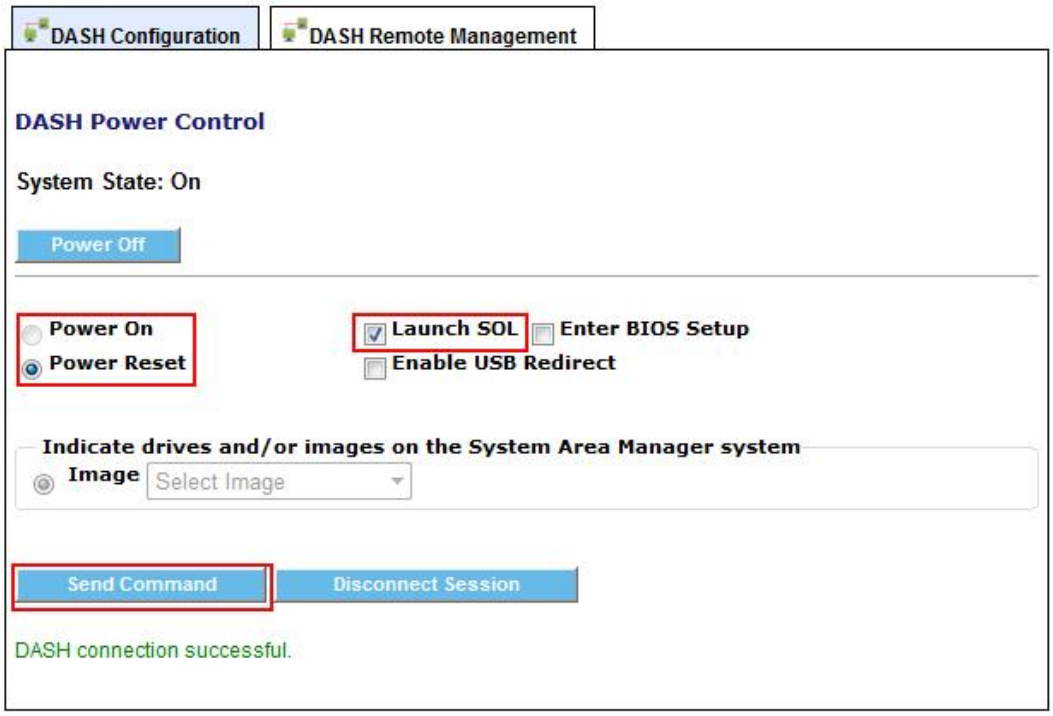

## DASH Serial Over LAN

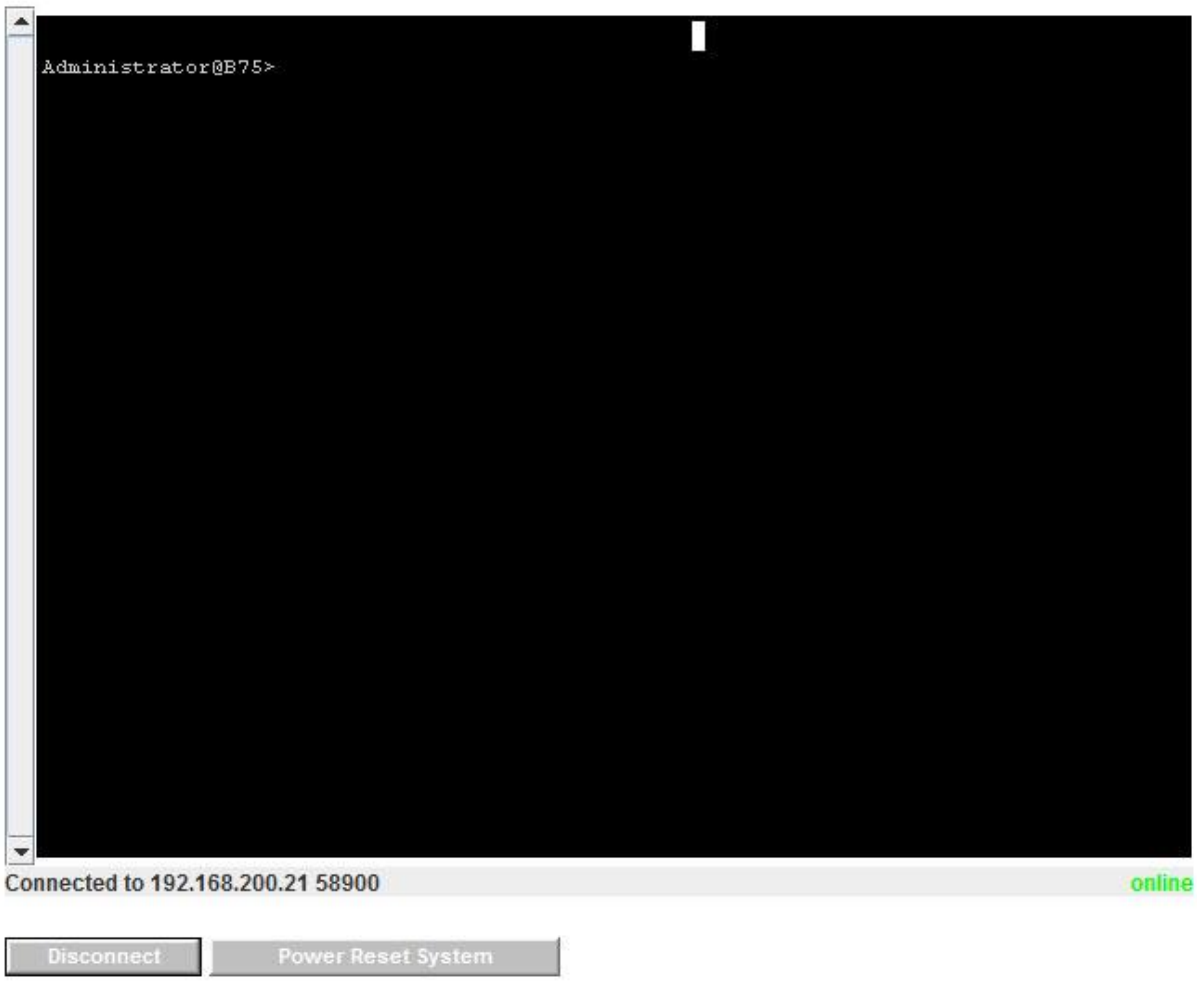
With Serial Over LAN you can access the system during its boot sequence, enabling you to access the system BIOS to make any needed changes.

Serial Over LAN is only available as the system powers on. The operating system GUI will not be displayed.

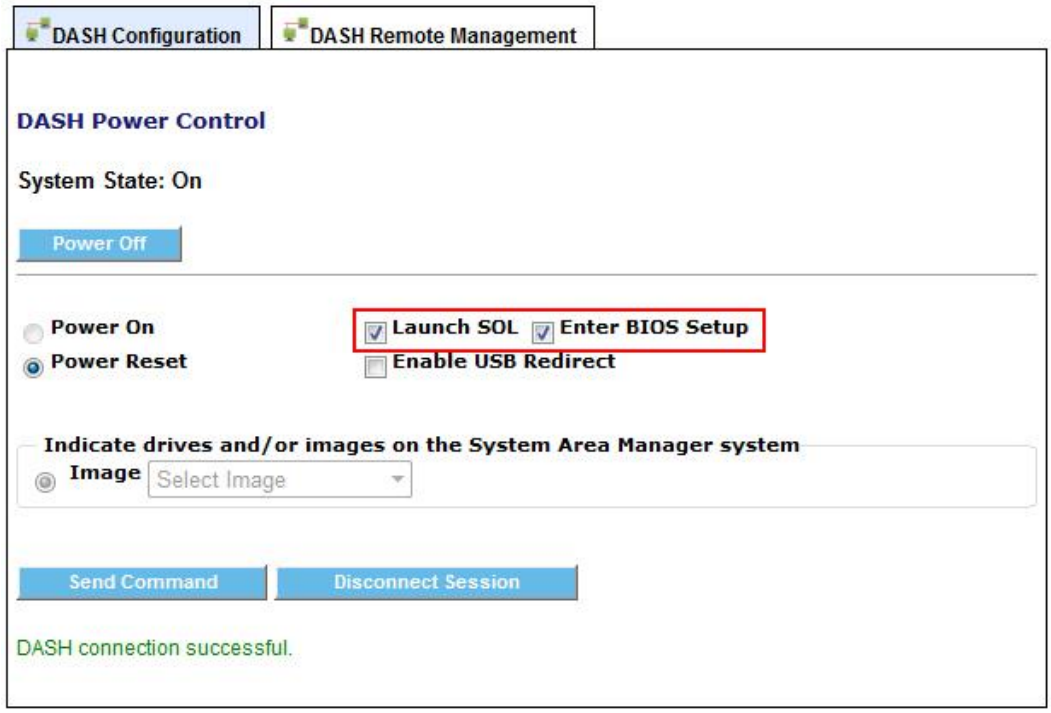
1. On the DASH Remote Management tab, establish a connection.
2. If the System State is Off, click the Power On radio button, or if the System State is On, click the Power Reset radio button. Check the box to Launch SOL. Click the Send Command button.

4. The Serial Over LAN console will be displayed in your web browser. Click on the console and press the BIOS access key (for example, F2 or DEL) to enter the BIOS setup when the message comes up. Should you need to reboot, you can click the Power Reset System button.


DASH Configuration
DASH Remote Management
DASH Power Control
System State: On
Power Off
Power On
Power Reset
Launch SOL
Enter BIOS Setup
Enable USB Redirect
Indicate drives and/or images on the System Area Manager system
Image
Select Image
Send Command
Disconnect Session
DASH connection successful.




4. You can also go directly into BIOS configuration by checking the Enter BIOS Setup box when launching Serial Over LAN.



## DASH USB Redirection

With System Area Manager and the DASH configured managed system, you can redirect media from the Area Manager system to the client system by using the USB Redirect feature in the DASH Remote Management tab.

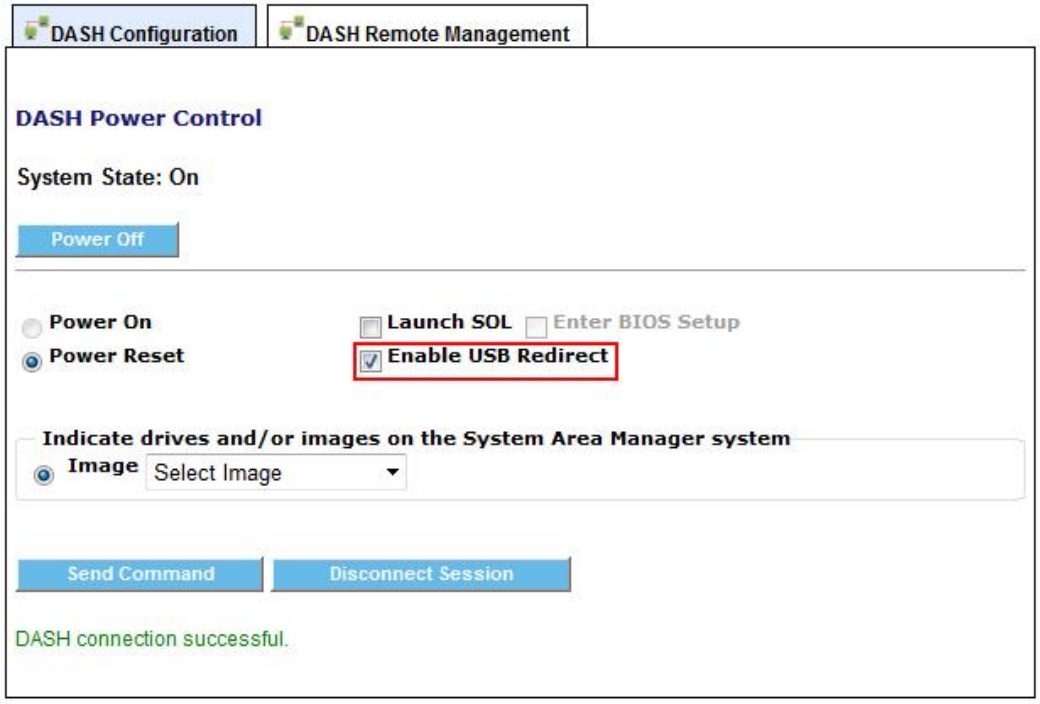
USB redirection is available as the system powers on. This allows you to boot from .IMG or .ISO bootable images.

In addition, USB redirection can be used when the system OS is running, and the image can be accessed as if it were physically connected to the client system.

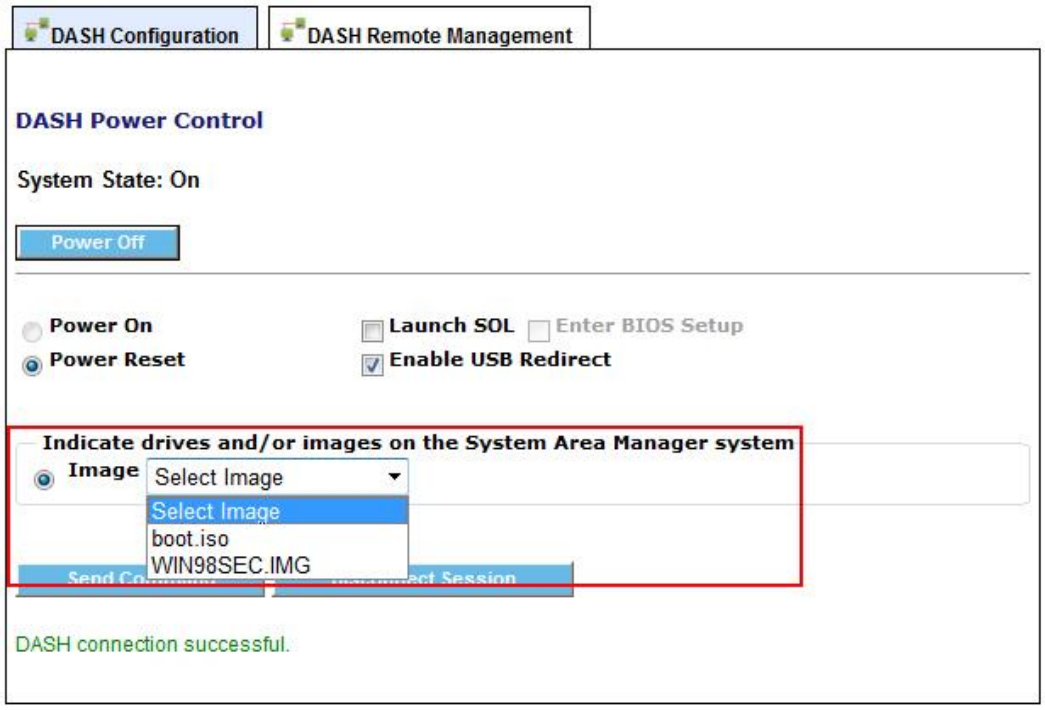
To make image files available for USB redirection, place them in the following folder on the System Area Manager:

***C:\SyAM\Jetty\syam\webapps\root\dashiso***

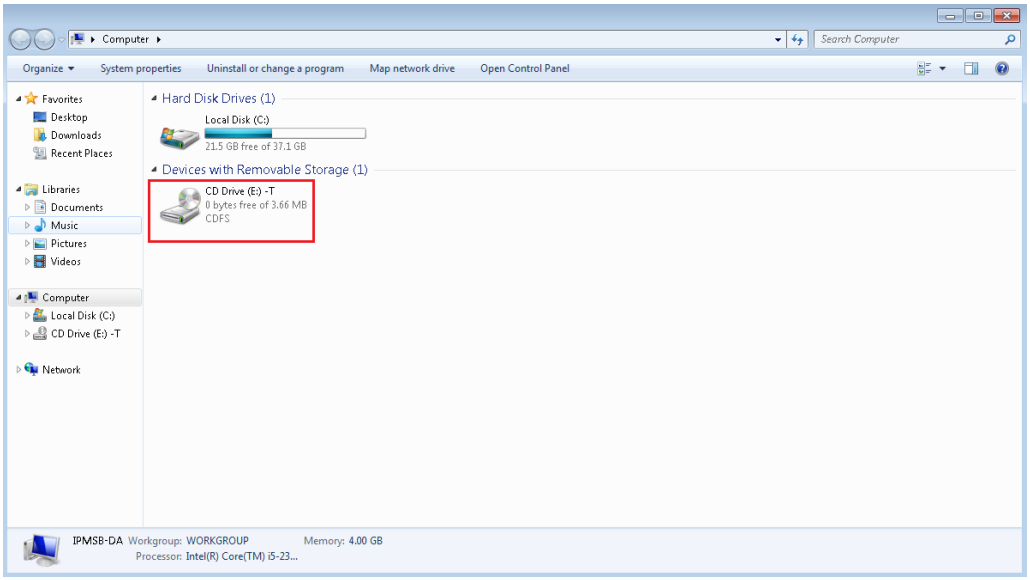
1. On the DASH Remote Management tab, establish a connection.
2. Check the box to Enable USB Redirect.



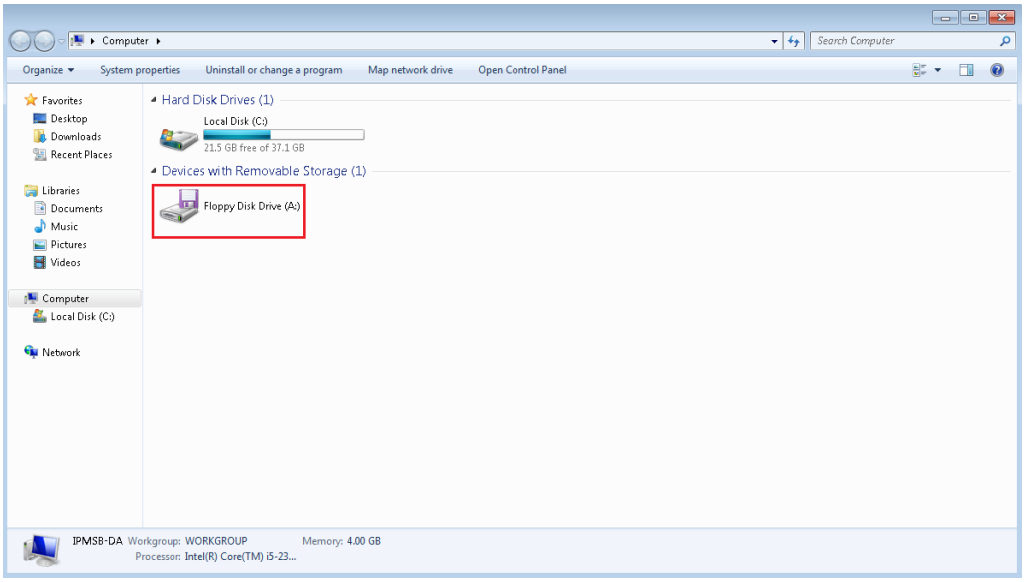

3. In the Image drop down menu, select the IMG or ISO image that will be redirected to the client system, then click the Send Command button. This will then redirect the image to the client system, where the files on that image can be accessed.




ISO images will appear as CD devices on the Windows client system.

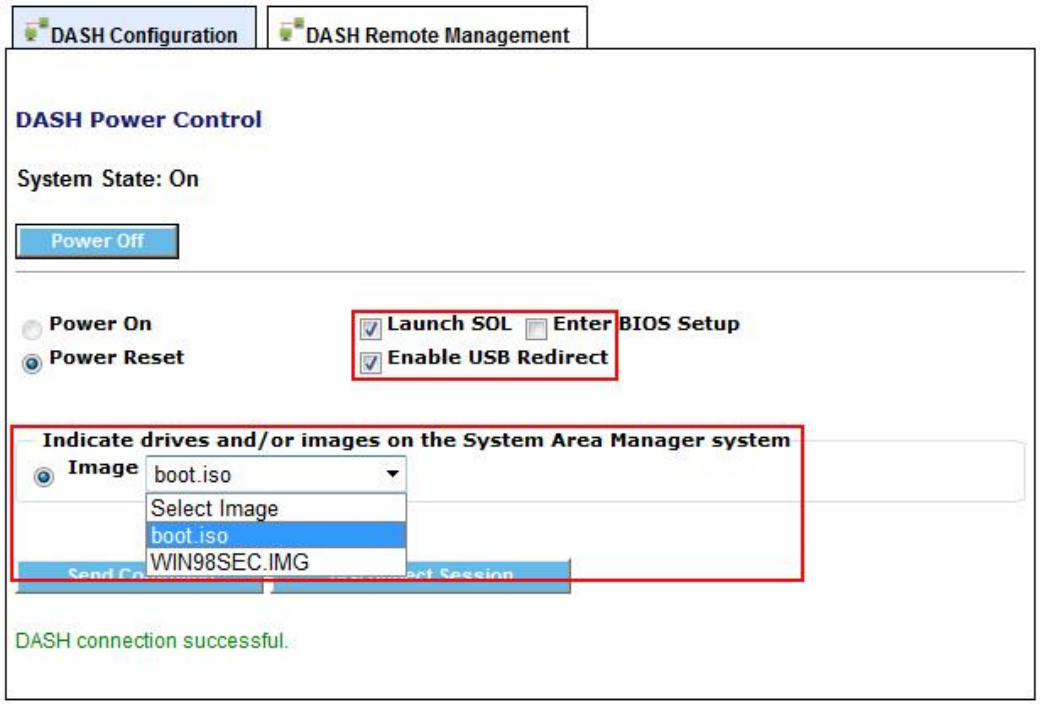



IMG images will appear as floppy disks on the Windows client system.



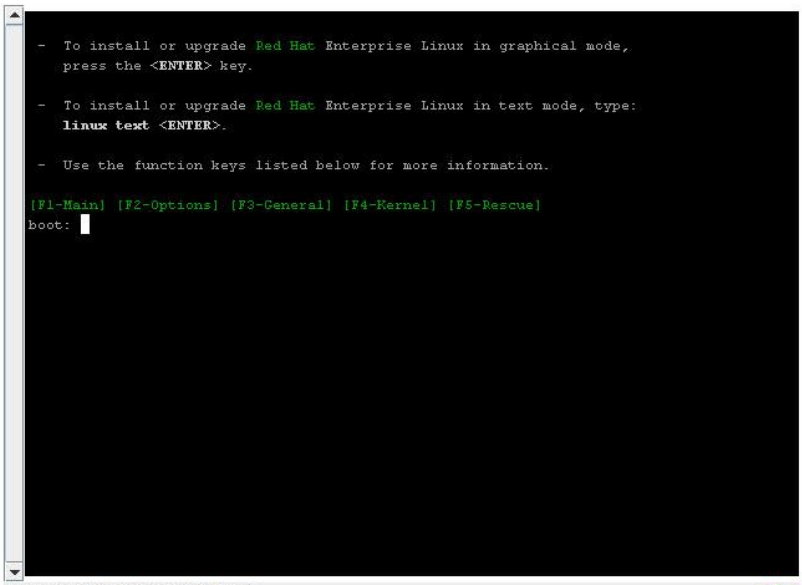

USB redirection can be used with Serial Over LAN so that the user can see the boot sequence and can take control of the boot with the ISO or IMG image. The BIOS boot order must have the CD/DVD before the hard drive for USB redirection to ISO when booting the system.

1. On the DASH Remote Management tab, establish a connection.
2. Choose the Power On or the Power Reset radio button.
3. Check the Launch SOL and Enable USB Redirect checkboxes.




4. In the Image drop down menu, select the IMG or ISO image that will be redirected to the client system, then click the Send Command button. This will then redirect the image to the client system, which will boot from the image.

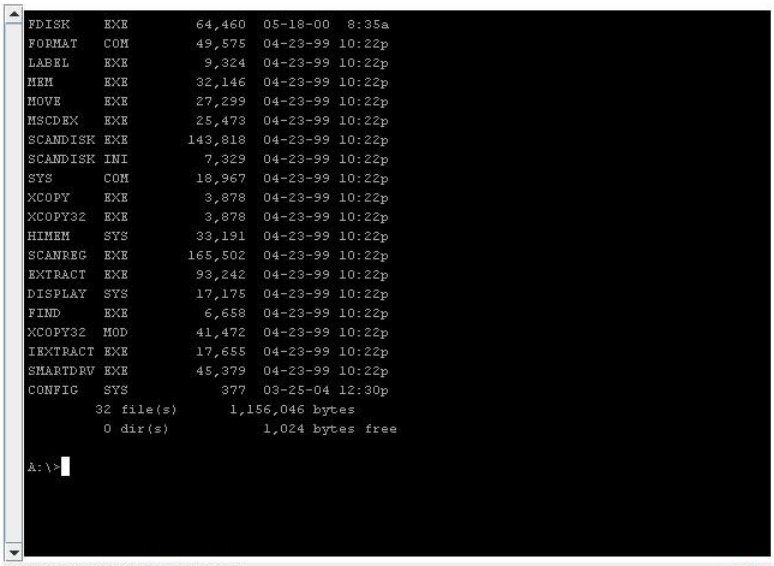
USB Redirect Image: http://192.168.200.21:3930/dashiso/boot.iso




Connected to 192.168.200.21 58900 online

Disconnect | Power Reset System

USB Redirect Image: http://192.168.200.21:3930/dashiso/WIN98SEC.IMG




Connected to 192.168.200.21 58900 online

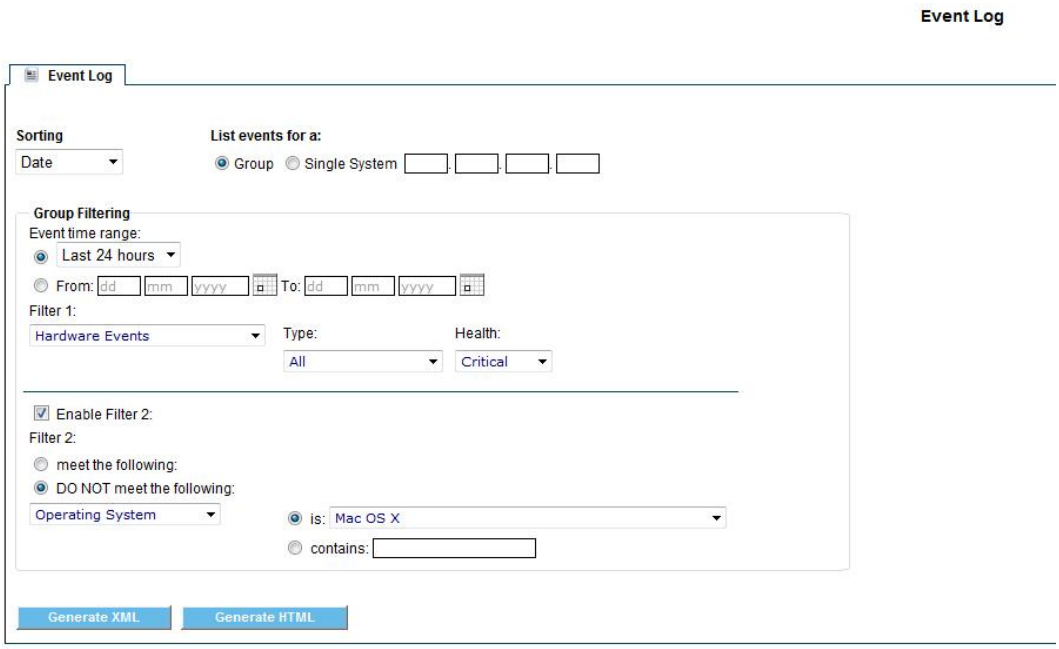
Disconnect | Power Reset System

# Chapter 6: Central Event Logging

All systems being managed by System Area Manager (systems present in the Management Tree) have their events automatically recorded in the System Area Manager Event Log. Each event is dated, and lists the location of the event by system name, IP address, and category (storage, network, hardware, etc.)

# Event Filtering

The Event Log screen provides sorting and filtering options for viewing events.




Choose the Sorting

- Date
- Event Type
- Host Name
- IP Address

Group or Single System IP Address

Time Range

- Last 24 Hours
- Last 7 Days
- Last 30 days
- All
- Or choose a Date Range (From – To)

Next you can choose from Filter 1:

- All Events
- Asset Monitoring Events
- Hardware Events
- Logical Disk Utilization Events

- Network Events
- Operator Events
- Performance Utilization Events
- Platform Event Traps
- Storage Events
- System Absent Events

You can then set a second filter by clicking the Enable Filter 2 check box.

This filter can be set to select events that meet or that DO NOT meet the following criteria:

- Asset Number
- Board Model
- Function
- Health
- Installed Applications
- Location
- Logical Free Disk Space
- Machine Model
- Operating System
- Owner
- Physical Disks
- Physical Memory
- Processor Model

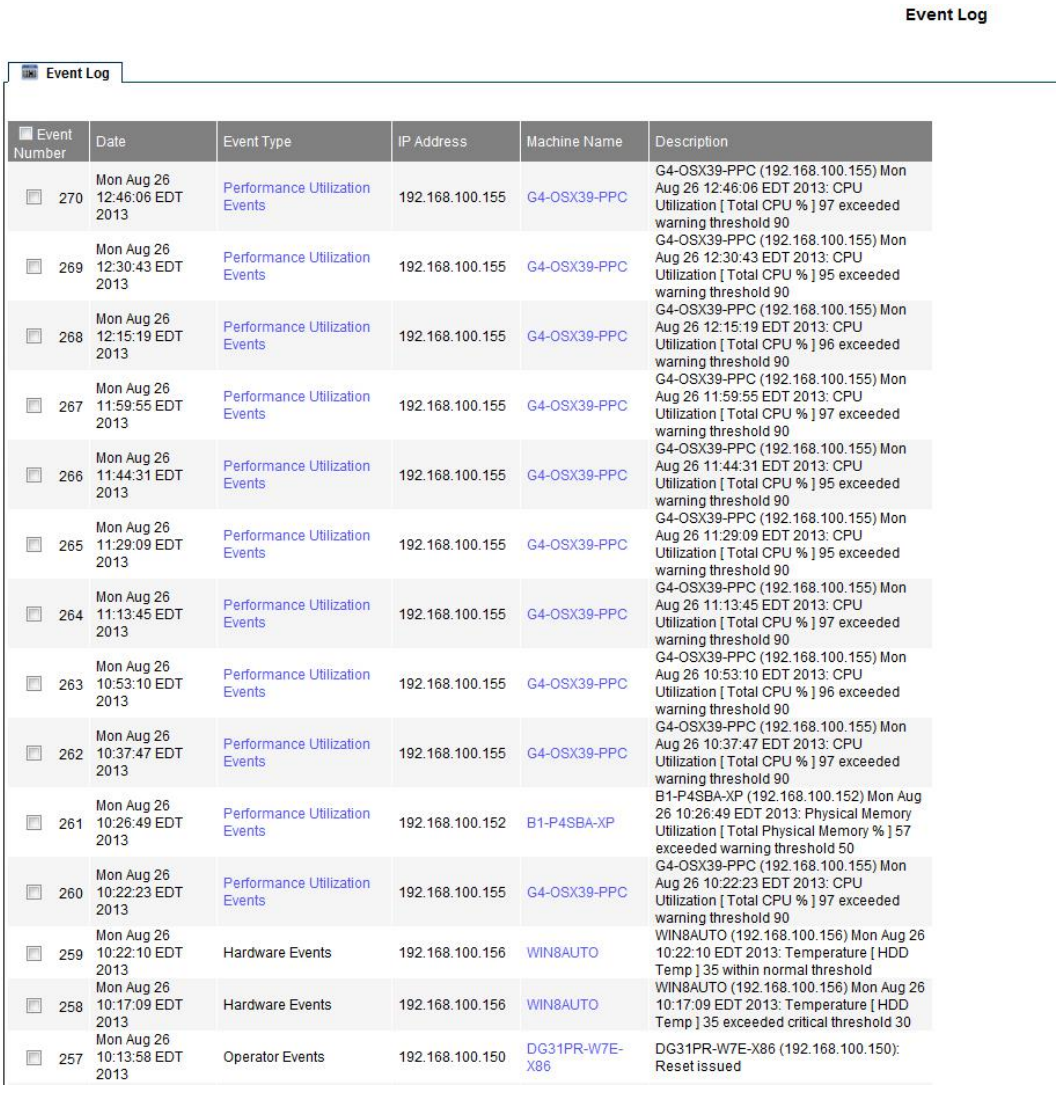
Once you have set the filter options you can either display the results on screen by pressing the Generate HTML button, or export them to XML by pressing the Generate XML button.

# Viewing Events

Once you click the Generate HTML button a new page is opened showing the events within your filtered criteria.

Ten events are shown per page and you can go to the Next page or Back a page by pressing the arrows at the bottom of the page.

If a Performance Utilization Event has occurred you can click on the event type to open up the processes snap shot. This will be in Memory order for a Physical or Virtual Memory Utilization event or CPU order for a CPU Utilization event.

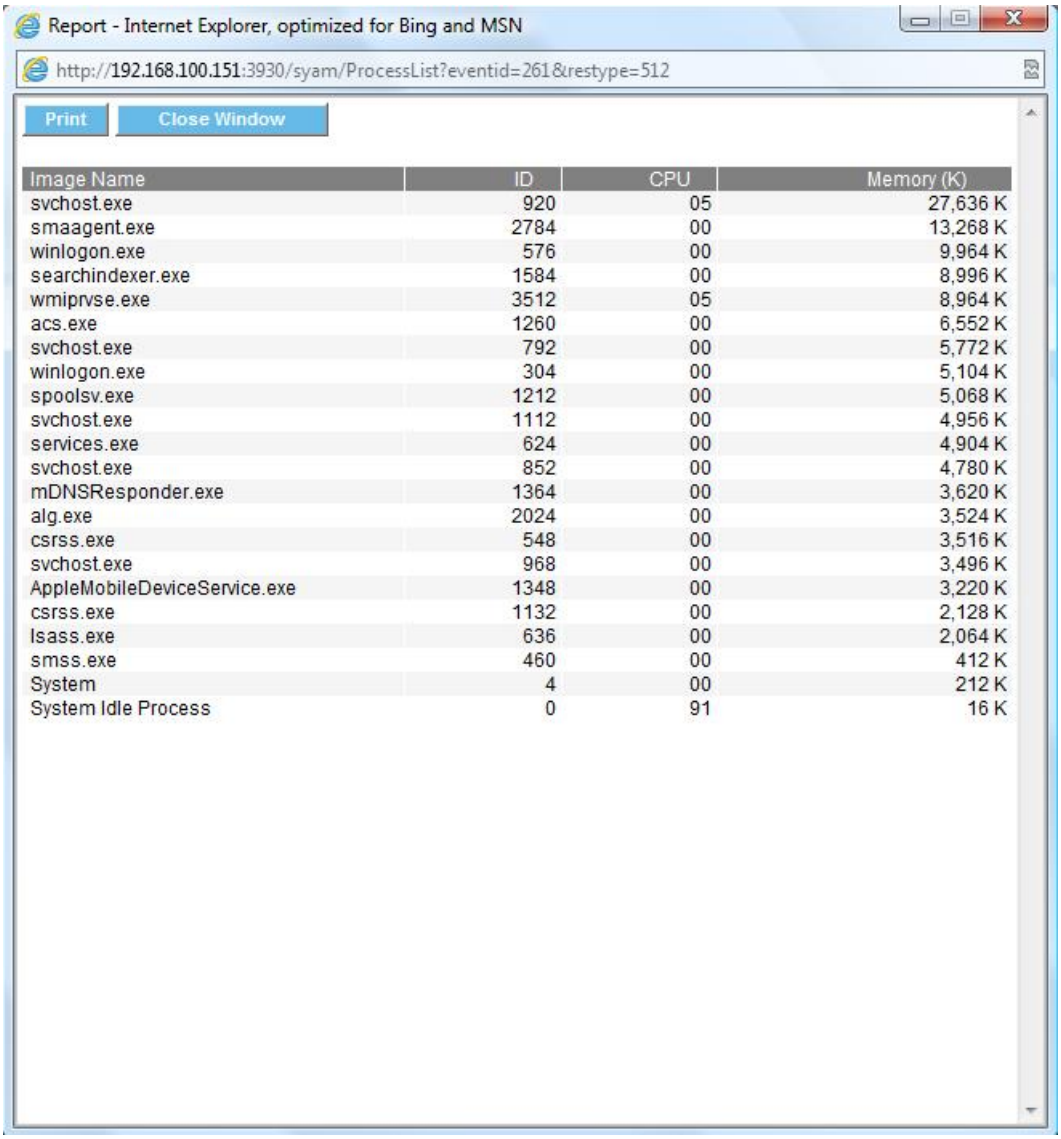


**Event Log**

Event Log

| Event Number | Date | Event Type | IP Address | Machine Name | Description |
|---|---|---|---|---|---|
| 270 | Mon Aug 26 12:46:06 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 12:46:06 EDT 2013: CPU Utilization [ Total CPU % ] 97 exceeded warning threshold 90 |
| 269 | Mon Aug 26 12:30:43 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 12:30:43 EDT 2013: CPU Utilization [ Total CPU % ] 95 exceeded warning threshold 90 |
| 268 | Mon Aug 26 12:15:19 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 12:15:19 EDT 2013: CPU Utilization [ Total CPU % ] 96 exceeded warning threshold 90 |
| 267 | Mon Aug 26 11:59:55 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 11:59:55 EDT 2013: CPU Utilization [ Total CPU % ] 97 exceeded warning threshold 90 |
| 266 | Mon Aug 26 11:44:31 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 11:44:31 EDT 2013: CPU Utilization [ Total CPU % ] 95 exceeded warning threshold 90 |
| 265 | Mon Aug 26 11:29:09 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 11:29:09 EDT 2013: CPU Utilization [ Total CPU % ] 95 exceeded warning threshold 90 |
| 264 | Mon Aug 26 11:13:45 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 11:13:45 EDT 2013: CPU Utilization [ Total CPU % ] 97 exceeded warning threshold 90 |
| 263 | Mon Aug 26 10:53:10 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 10:53:10 EDT 2013: CPU Utilization [ Total CPU % ] 96 exceeded warning threshold 90 |
| 262 | Mon Aug 26 10:37:47 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 10:37:47 EDT 2013: CPU Utilization [ Total CPU % ] 97 exceeded warning threshold 90 |
| 261 | Mon Aug 26 10:26:49 EDT 2013 | Performance Utilization Events | 192.168.100.152 | B1-P4SBA-XP | B1-P4SBA-XP (192.168.100.152) Mon Aug 26 10:26:49 EDT 2013: Physical Memory Utilization [ Total Physical Memory % ] 57 exceeded warning threshold 50 |
| 260 | Mon Aug 26 10:22:23 EDT 2013 | Performance Utilization Events | 192.168.100.155 | G4-OSX39-PPC | G4-OSX39-PPC (192.168.100.155) Mon Aug 26 10:22:23 EDT 2013: CPU Utilization [ Total CPU % ] 97 exceeded warning threshold 90 |
| 259 | Mon Aug 26 10:22:10 EDT 2013 | Hardware Events | 192.168.100.156 | WIN8AUTO | WIN8AUTO (192.168.100.156) Mon Aug 26 10:22:10 EDT 2013: Temperature [ HDD Temp ] 35 within normal threshold |
| 258 | Mon Aug 26 10:17:09 EDT 2013 | Hardware Events | 192.168.100.156 | WIN8AUTO | WIN8AUTO (192.168.100.156) Mon Aug 26 10:17:09 EDT 2013: Temperature [ HDD Temp ] 35 exceeded critical threshold 30 |
| 257 | Mon Aug 26 10:13:58 EDT 2013 | Operator Events | 192.168.100.150 | DG31PR-W7E-X86 | DG31PR-W7E-X86 (192.168.100.150): Reset issued |

By clicking the Utilization Event you can review the details process list that was taken when the issue was identified.




| Image Name | ID | CPU | Memory (K) |
|---|---|---|---|
| svchost.exe | 920 | 05 | 27,636 K |
| smaagent.exe | 2784 | 00 | 13,268 K |
| winlogon.exe | 576 | 00 | 9,964 K |
| searchindexer.exe | 1584 | 00 | 8,996 K |
| wmiprvse.exe | 3512 | 05 | 8,964 K |
| acs.exe | 1260 | 00 | 6,552 K |
| svchost.exe | 792 | 00 | 5,772 K |
| winlogon.exe | 304 | 00 | 5,104 K |
| spoolsv.exe | 1212 | 00 | 5,068 K |
| svchost.exe | 1112 | 00 | 4,956 K |
| services.exe | 624 | 00 | 4,904 K |
| svchost.exe | 852 | 00 | 4,780 K |
| mDNSResponder.exe | 1364 | 00 | 3,620 K |
| alg.exe | 2024 | 00 | 3,524 K |
| csrss.exe | 548 | 00 | 3,516 K |
| svchost.exe | 968 | 00 | 3,496 K |
| AppleMobileDeviceService.exe | 1348 | 00 | 3,220 K |
| csrss.exe | 1132 | 00 | 2,128 K |
| lsass.exe | 636 | 00 | 2,064 K |
| smss.exe | 460 | 00 | 412 K |
| System | 4 | 00 | 212 K |
| System Idle Process | 0 | 91 | 16 K |

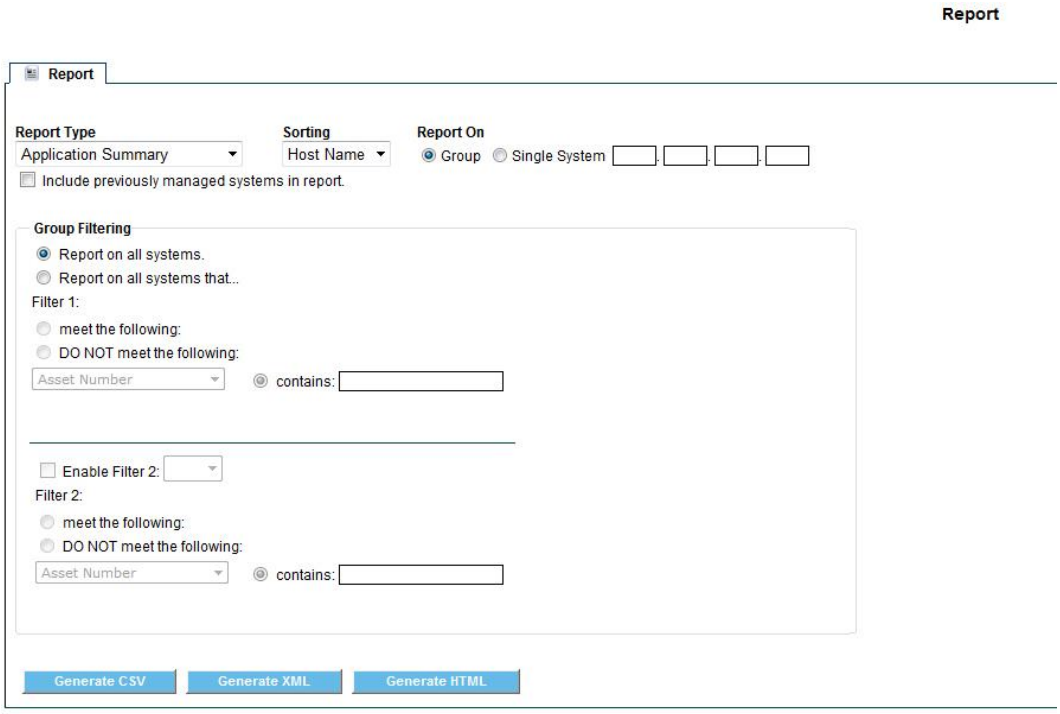
## Deleting Events from the Event Log

You can remove events from the event log by clicking on their check box and pressing the Deleted Selected Events button. You can choose all events on the page by clicking on the check box in the header bar next to Event Number.

# Chapter 7: Central Reporting

Users of System Area Manager can run a variety of reports on the managed systems being monitored. The information can be viewed on-screen, printed, or exported to files in CSV or XML format. Sorting and filtering options are provided for all reports.

The System Area Manager database includes data on systems that have been removed and are no longer under management. Check the box to include information on previously managed systems in a report.




## Report Types

There are 10 different report types to choose from:

- Application Summary
- Asset Details
- Asset List
- Asset Summary
- Operating System Summary
- User Audit
- Local Alert
- Application Utilization
- Power Hours Summary
- Power Hours Detail

The administrator can hide the Application Utilization report so it is not displayed in the menu. In the folder `C:\SyAM\Jetty\syam\webapps\root\WEB-INF\` edit the file `syam.properties` setting the value `enable_app_util=false`. After editing the file, the SyAM System Area Manager Web Server service must be restarted.

## Report Filtering

To enable Filter 1, the primary report filter, click the radio button to “Report on all systems that…”, then set the sense of the filter by clicking “meet the following” or “DO NOT meet the following”, then use the drop down menu to select the filtering parameter. The filtering options provided will vary according to the particular report.

To use an additional filter, check the “Enable Filter 2” box, then use the drop down menu to set the relationship (“And” or “Or”) between the two filters. Set the sense of the filter and choose the filtering parameter in the same way as Filter 1.

# Application Summary Report

The Application Summary Report contains the following information:

- Application Name
- Version
- Vendor
- Total quantity installed

The report can be sorted by Host Name or by IP Address.

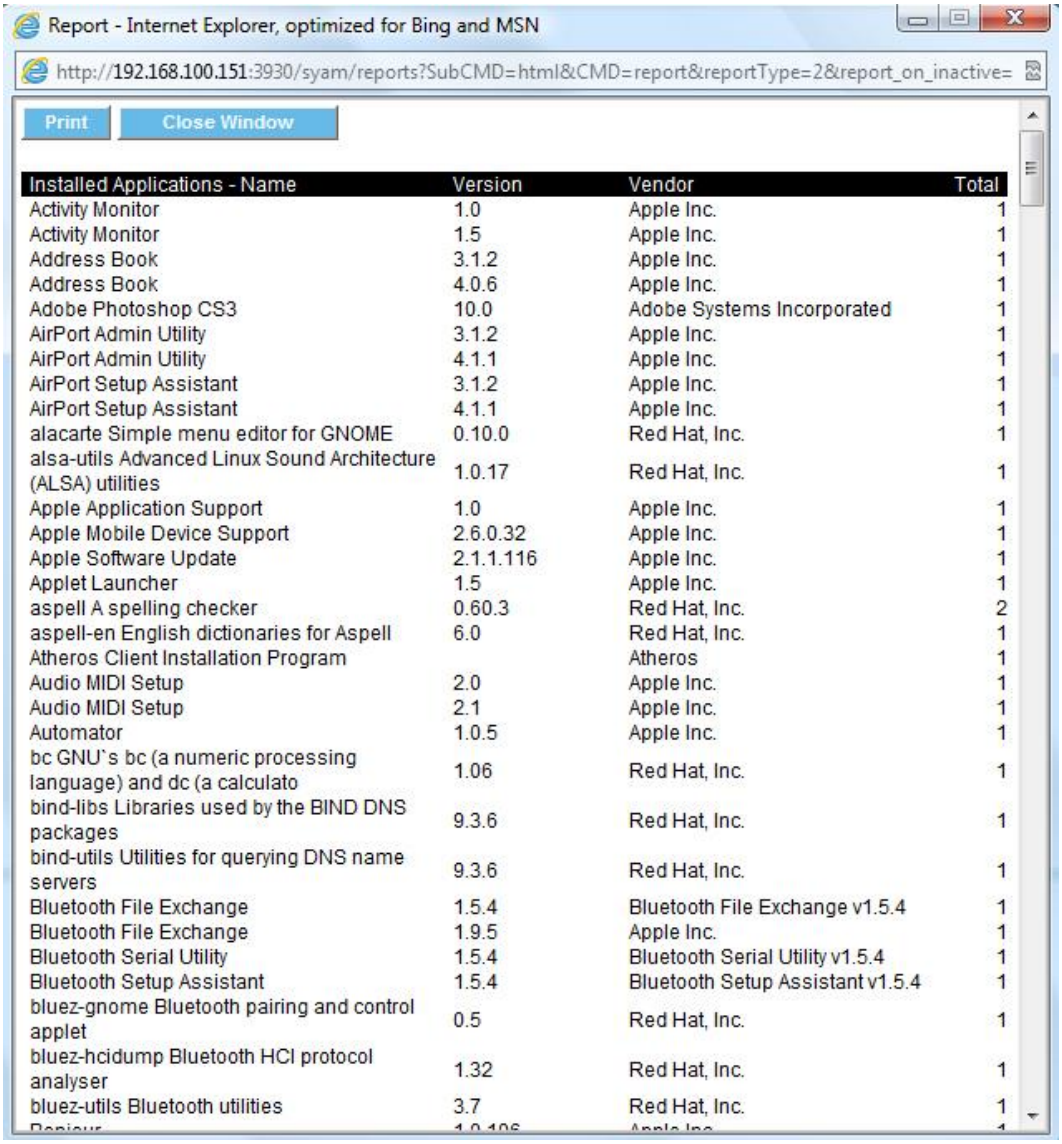
Report on a single machine by clicking the Single System radio button and entering an IP address. Report on all machines by clicking the Group radio button and the “Report on all systems” button. Report on selected machines by clicking the Group radio button and enabling Filter 1, and optionally, Filter 2.

Filter 1 options for this report:

- Operating System
- Location
- Function
- Health
- Installed Applications
- Logical Disk Free Space
- Asset Number
- Owner
- Machine Model
- Board Model
- Physical Disks
- Physical Memory
- Processor Model
- Machine Name
- Unresponsive For

Filter 2 options for this report:

- Operating System
- Location
- Function
- Health
- Installed Applications
- Logical Disk Free Space
- Asset Number
- Owner
- Machine Model
- Board Model
- Physical Disks
- Physical Memory
- Processor Model
- Machine Name




| Installed Applications - Name | Version | Vendor | Total |
|---|---|---|---|
| Activity Monitor | 1.0 | Apple Inc. | 1 |
| Activity Monitor | 1.5 | Apple Inc. | 1 |
| Address Book | 3.1.2 | Apple Inc. | 1 |
| Address Book | 4.0.6 | Apple Inc. | 1 |
| Adobe Photoshop CS3 | 10.0 | Adobe Systems Incorporated | 1 |
| AirPort Admin Utility | 3.1.2 | Apple Inc. | 1 |
| AirPort Admin Utility | 4.1.1 | Apple Inc. | 1 |
| AirPort Setup Assistant | 3.1.2 | Apple Inc. | 1 |
| AirPort Setup Assistant | 4.1.1 | Apple Inc. | 1 |
| alacarte Simple menu editor for GNOME | 0.10.0 | Red Hat, Inc. | 1 |
| alsa-utils Advanced Linux Sound Architecture (ALSA) utilities | 1.0.17 | Red Hat, Inc. | 1 |
| Apple Application Support | 1.0 | Apple Inc. | 1 |
| Apple Mobile Device Support | 2.6.0.32 | Apple Inc. | 1 |
| Apple Software Update | 2.1.1.116 | Apple Inc. | 1 |
| Applet Launcher | 1.5 | Apple Inc. | 1 |
| aspell A spelling checker | 0.60.3 | Red Hat, Inc. | 2 |
| aspell-en English dictionaries for Aspell | 6.0 | Red Hat, Inc. | 1 |
| Atheros Client Installation Program | | Atheros | 1 |
| Audio MIDI Setup | 2.0 | Apple Inc. | 1 |
| Audio MIDI Setup | 2.1 | Apple Inc. | 1 |
| Automator | 1.0.5 | Apple Inc. | 1 |
| bc GNU`s bc (a numeric processing language) and dc (a calculato | 1.06 | Red Hat, Inc. | 1 |
| bind-libs Libraries used by the BIND DNS packages | 9.3.6 | Red Hat, Inc. | 1 |
| bind-utils Utilities for querying DNS name servers | 9.3.6 | Red Hat, Inc. | 1 |
| Bluetooth File Exchange | 1.5.4 | Bluetooth File Exchange v1.5.4 | 1 |
| Bluetooth File Exchange | 1.9.5 | Apple Inc. | 1 |
| Bluetooth Serial Utility | 1.5.4 | Bluetooth Serial Utility v1.5.4 | 1 |
| Bluetooth Setup Assistant | 1.5.4 | Bluetooth Setup Assistant v1.5.4 | 1 |
| bluez-gnome Bluetooth pairing and control applet | 0.5 | Red Hat, Inc. | 1 |
| bluez-hcidump Bluetooth HCI protocol analyser | 1.32 | Red Hat, Inc. | 1 |
| bluez-utils Bluetooth utilities | 3.7 | Red Hat, Inc. | 1 |
| Bonjour | 1.0.106 | Apple Inc. | 1 |

# Asset Details Report

The Asset Details Report contains the following information:

- Machine Name
- Health State
- IP Address
- Domain or Workgroup
- Operating System / OS Version / OS Service Pack
- Location / Function
- Asset Number / Value / Date Installed / Owner
- Machine Model / Serial Number / Inventory Number / Manufacturer
- Number of Logical CPUs
- Processor Model / Manufacturer / Clock Speed
- Board Model / Manufacturer / Serial Number
- BIOS Manufacturer / BIOS Release Date / SMBIOS Rev
- Maximum Supported Memory / Memory Slots
- Sensor Devices
- Display Adapter Model / Memory
- Monitor Name / Serial Number
- Memory Location / Size / Label
- Physical Memory Total / In Use
- Virtual Memory Total / In Use
- Physical Disks Device ID / Total Size / Device Information
- Logical Disks Name / Type / Free Space / Space Used / Total Size / Utilization
- RAID Controllers installed
- RAID Controller Model / Status / RAID Level / Capacity / # Drives
- Removable Device Name / Description
- Network Adapter Number / Description / DHCP / IP Address / MAC Address
- Slots - ID / Status
- Ports – Name / Speed
- Installed Applications – Name / Vendor / Version
- Installed Drivers – Name / Category / Version / Provider

The report can be sorted by Host Name or by IP Address.

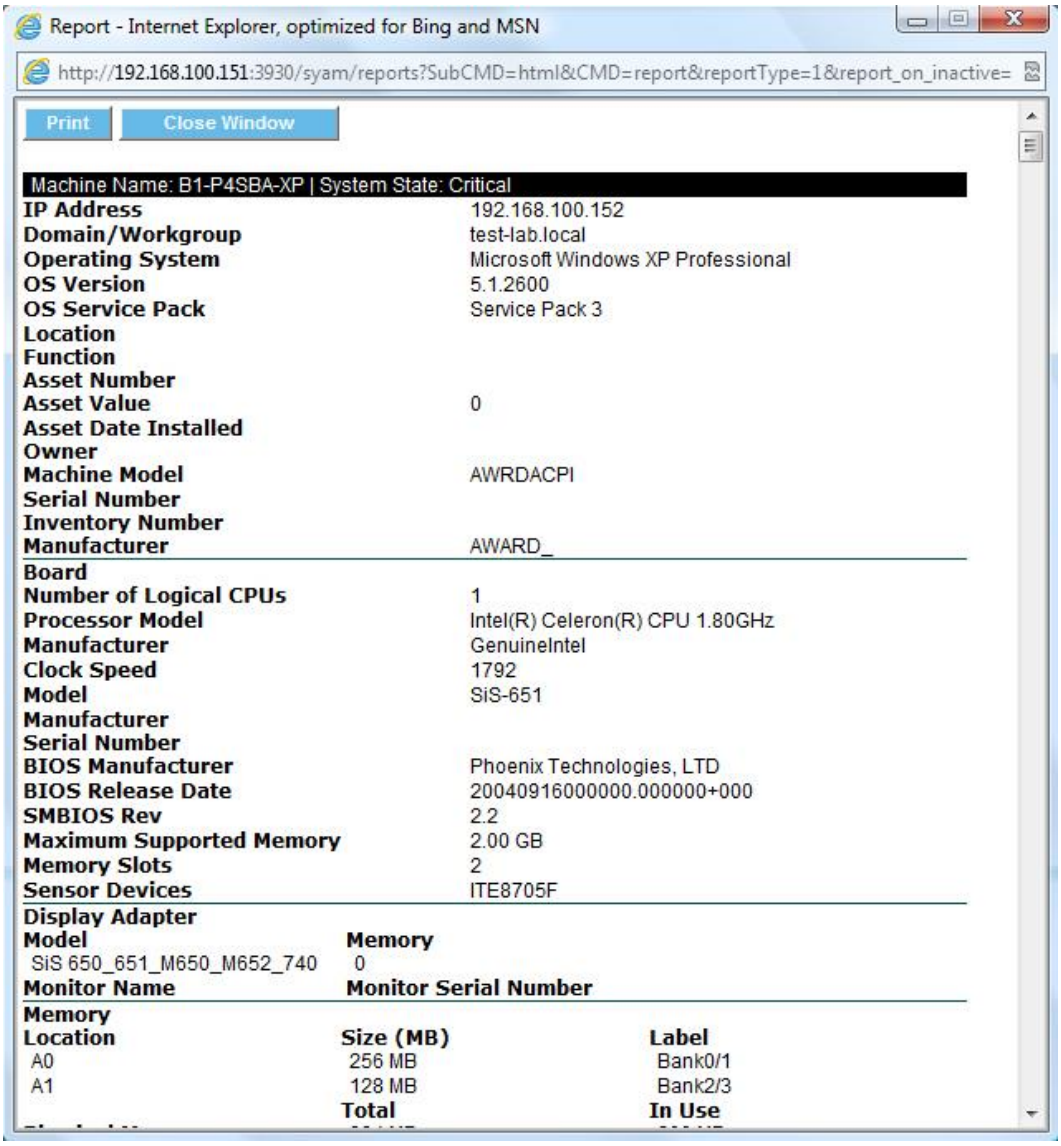
Report on a single machine by clicking the Single System radio button and entering an IP address. Report on all machines by clicking the Group radio button and the “Report on all systems” button. Report on selected machines by clicking the Group radio button and enabling Filter 1, and optionally, Filter 2.

Filter 1 options for this report:

- Asset Number
- Board Model
- Function
- Health
- Installed Applications
- Location
- Logical Disk Free Space
- Machine Model
- Machine Name
- Operating System
- Owner
- Physical Disks
- Physical Memory
- Processor Model
- Unresponsive For

Filter 2 options for this report:

- Asset Number
- Board Model
- Function
- Health
- Installed Applications
- Location
- Logical Disk Free Space
- Machine Model
- Machine Name
- Operating System
- Owner
- Physical Disks
- Physical Memory
- Processor Model


Report - Internet Explorer, optimized for Bing and MSN
http://192.168.100.151:3930/syam/reports?SubCMD=html&CMD=report&reportType=1&report_on_inactive=
Print
Close Window
Machine Name: B1-P4SBA-XP | System State: Critical
IP Address 192.168.100.152
Domain/Workgroup test-lab.local
Operating System Microsoft Windows XP Professional
OS Version 5.1.2600
OS Service Pack Service Pack 3
Location
Function
Asset Number
Asset Value 0
Asset Date Installed
Owner
Machine Model AWRDACPI
Serial Number
Inventory Number
Manufacturer AWARD_
Board
Number of Logical CPUs 1
Processor Model Intel(R) Celeron(R) CPU 1.80GHz
Manufacturer GenuineIntel
Clock Speed 1792
Model SiS-651
Manufacturer
Serial Number
BIOS Manufacturer Phoenix Technologies, LTD
BIOS Release Date 20040916000000.000000+000
SMBIOS Rev 2.2
Maximum Supported Memory 2.00 GB
Memory Slots 2
Sensor Devices ITE8705F
Display Adapter
Model Memory
SiS 650_651_M650_M652_740 0
Monitor Name Monitor Serial Number
Memory
Location Size (MB) Label
A0 256 MB Bank0/1
A1 128 MB Bank2/3
Total In Use

# Asset List Report

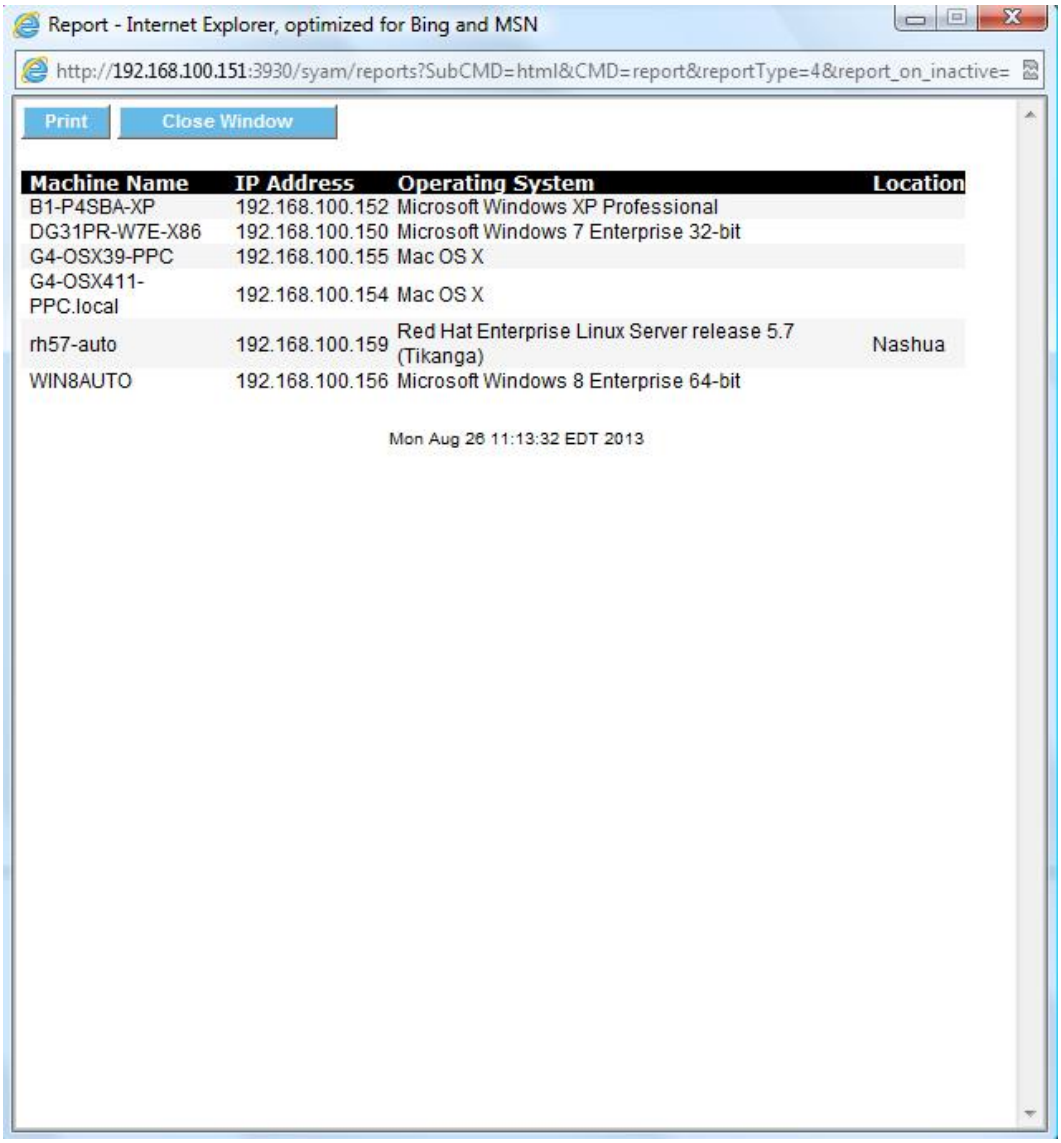
The Asset List Report contains the following information:

- Machine Name
- IP Address
- Operating System
- Location

The report can be sorted by Host Name or by IP Address.

Report on a single machine by clicking the Single System radio button and entering an IP address. Report on all machines by clicking the Group radio button and the “Report on all systems” button. Report on selected machines by clicking the Group radio button and enabling Filter 1, and optionally, Filter 2.

Filter 1 and Filter 2 options for this report are the same as for the Asset Details Report.



# Asset Summary Report

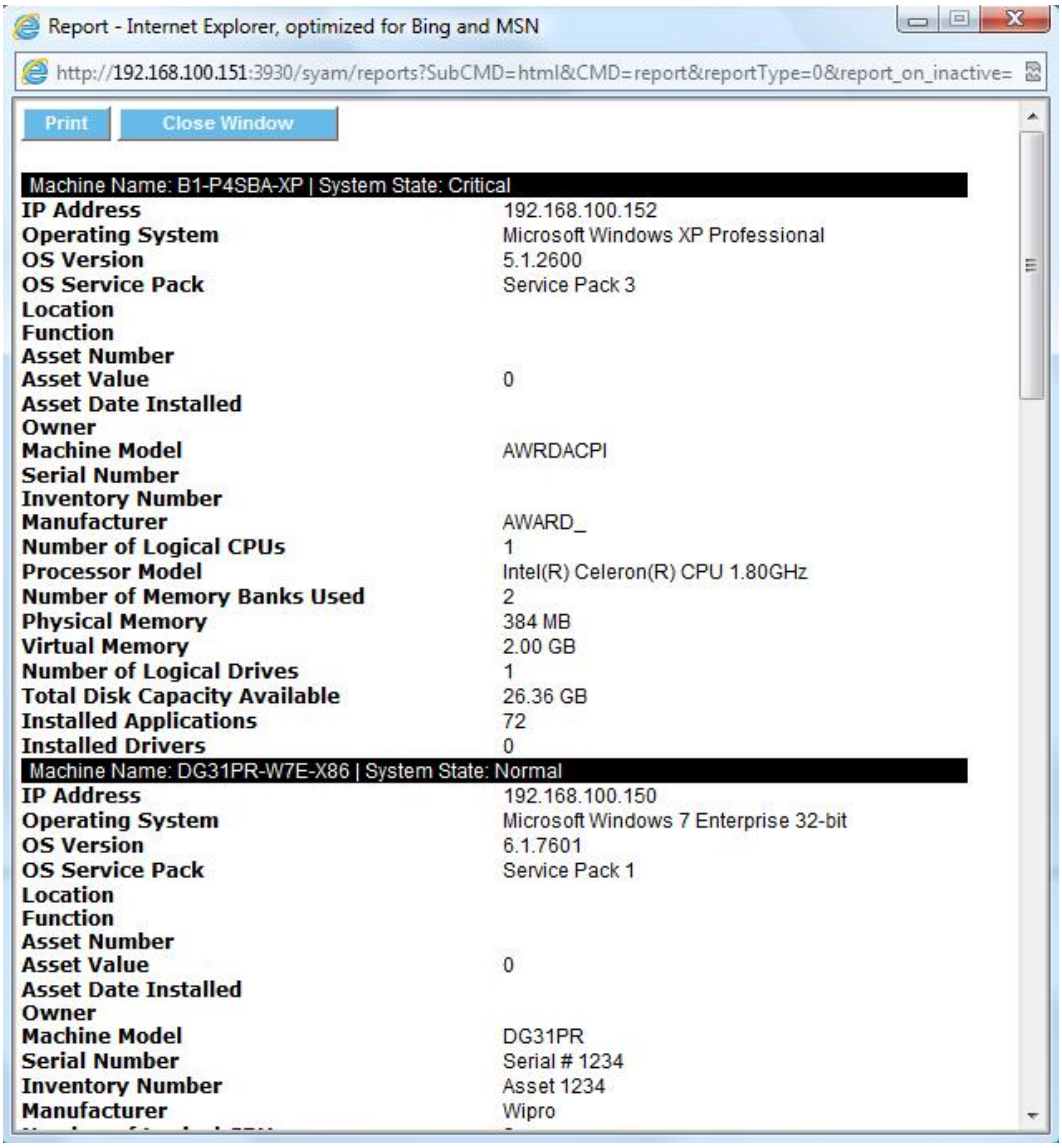
The Asset Summary Report contains the following information:

- Machine Name
- Health State
- IP Address
- Operating System / OS Version / OS Service Pack
- Location / Function
- Asset Number / Value / Date Installed / Owner
- Machine Model / Serial Number / Inventory Number / Manufacturer
- Number of Logical CPUs and type
- Total amount of Physical and Virtual Memory installed and number of memory banks used
- Number of Logical Disks and capacity available
- RAID Controllers installed
- Number of Installed Applications
- Number of Installed Drivers

The report can be sorted by Host Name or by IP Address.

Report on a single machine by clicking the Single System radio button and entering an IP address. Report on all machines by clicking the Group radio button and the “Report on all systems” button. Report on selected machines by clicking the Group radio button and enabling Filter 1, and optionally, Filter 2.

Filter 1 and Filter 2 options for this report are the same as for the Asset Details Report.




| Machine Name: B1-P4SBA-XP \| System State: Critical | |
|---|---|
| **IP Address** | 192.168.100.152 |
| **Operating System** | Microsoft Windows XP Professional |
| **OS Version** | 5.1.2600 |
| **OS Service Pack** | Service Pack 3 |
| **Location** | |
| **Function** | |
| **Asset Number** | |
| **Asset Value** | 0 |
| **Asset Date Installed** | |
| **Owner** | |
| **Machine Model** | AWRDACPI |
| **Serial Number** | |
| **Inventory Number** | |
| **Manufacturer** | AWARD_ |
| **Number of Logical CPUs** | 1 |
| **Processor Model** | Intel(R) Celeron(R) CPU 1.80GHz |
| **Number of Memory Banks Used** | 2 |
| **Physical Memory** | 384 MB |
| **Virtual Memory** | 2.00 GB |
| **Number of Logical Drives** | 1 |
| **Total Disk Capacity Available** | 26.36 GB |
| **Installed Applications** | 72 |
| **Installed Drivers** | 0 |
| Machine Name: DG31PR-W7E-X86 \| System State: Normal | |
| **IP Address** | 192.168.100.150 |
| **Operating System** | Microsoft Windows 7 Enterprise 32-bit |
| **OS Version** | 6.1.7601 |
| **OS Service Pack** | Service Pack 1 |
| **Location** | |
| **Function** | |
| **Asset Number** | |
| **Asset Value** | 0 |
| **Asset Date Installed** | |
| **Owner** | |
| **Machine Model** | DG31PR |
| **Serial Number** | Serial # 1234 |
| **Inventory Number** | Asset 1234 |
| **Manufacturer** | Wipro |

# Operating System Summary Report

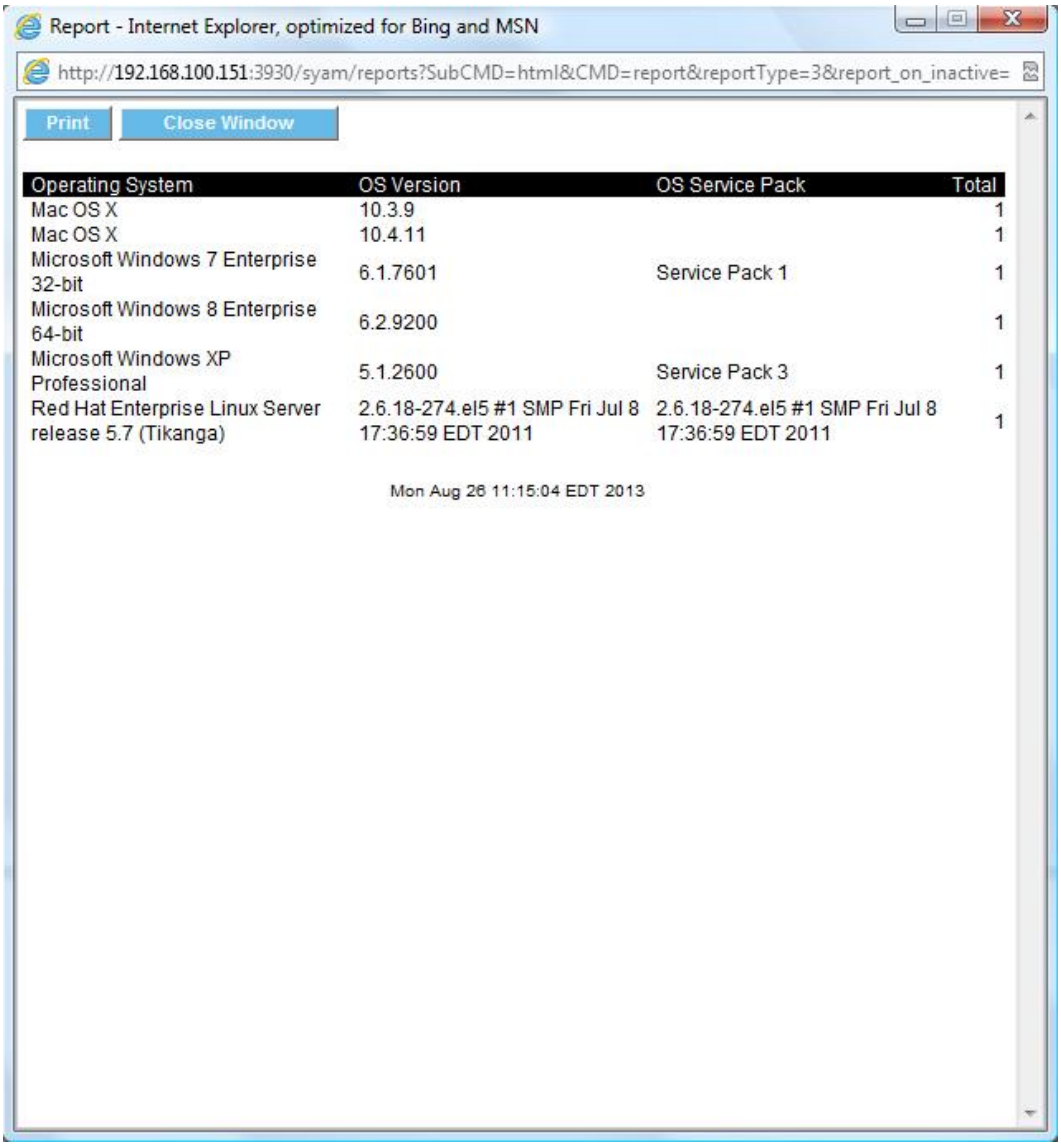
The Operating System Summary Report contains the following information:

- Operating System
- OS Version
- OS Service Pack
- Total Deployed

The report can be sorted by Host Name or by IP Address.

Report on a single machine by clicking the Single System radio button and entering an IP address. Report on all machines by clicking the Group radio button and the “Report on all systems” button. Report on selected machines by clicking the Group radio button and enabling Filter 1, and optionally, Filter 2.

Filter 1 and Filter 2 options for this report are the same as for the Asset Details Report.



# User Audit Report

The User Audit Report contains the following information:

- User Name
- Machine Name
- IP Address
- Domain or Workgroup
- Date
- Action

Choose the time period to be covered by the report, either by clicking the radio button for the drop down menu and making a selection from the menu (Last 24 hours, Last 7 days, Last 30 days, All) or by clicking the radio button to specify From – To and entering dates.

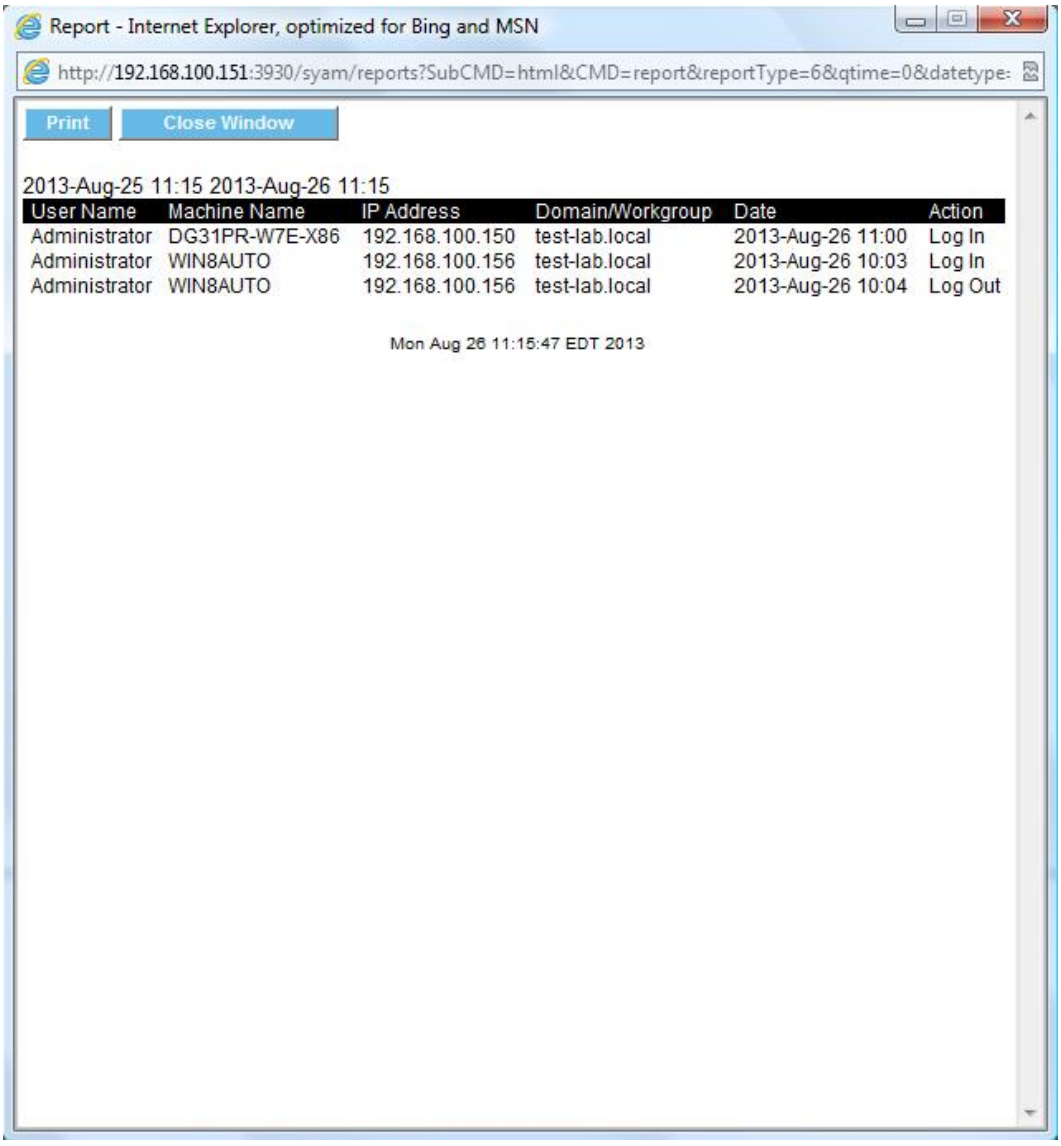
Report on all machines by clicking the “Report on all systems” radio button. Report on selected machines by enabling Filter 1, and optionally, Filter 2.

Filter 1 options for this report:

- User Name
- Machine Name

Filter 2 options for this report:

- Operating System
- Location
- Function
- Health
- Installed Applications
- Logical Disk Free Space
- Asset Number
- Owner
- Machine Model
- Board Model
- Physical Disks
- Physical Memory
- Processor Model
- Machine Name


Report - Internet Explorer, optimized for Bing and MSN
http://192.168.100.151:3930/syam/reports?SubCMD=html&CMD=report&reportType=6&qtime=0&datetype=
Print
Close Window
2013-Aug-25 11:15 2013-Aug-26 11:15
User Name Machine Name IP Address Domain/Workgroup Date Action
Administrator DG31PR-W7E-X86 192.168.100.150 test-lab.local 2013-Aug-26 11:00 Log In
Administrator WIN8AUTO 192.168.100.156 test-lab.local 2013-Aug-26 10:03 Log In
Administrator WIN8AUTO 192.168.100.156 test-lab.local 2013-Aug-26 10:04 Log Out
Mon Aug 26 11:15:47 EDT 2013

# Local Alert Report

The Local Alert Report contains the following information:

- Message
- Status
- Event Time
- Acknowledge Time
- Acknowledge User
- Acknowledge Domain
- Event Category
- Asset Type
- Asset Change

The report can be sorted by Date Alerted, Date Acknowledged, User Name, Machine Name, or IP Address.

Choose the time period to be covered by the report, either by clicking the radio button for the drop down menu and making a selection from the menu (Last 24 hours, Last 7 days, Last 30 days, All) or by clicking the radio button to specify From – To and entering dates.

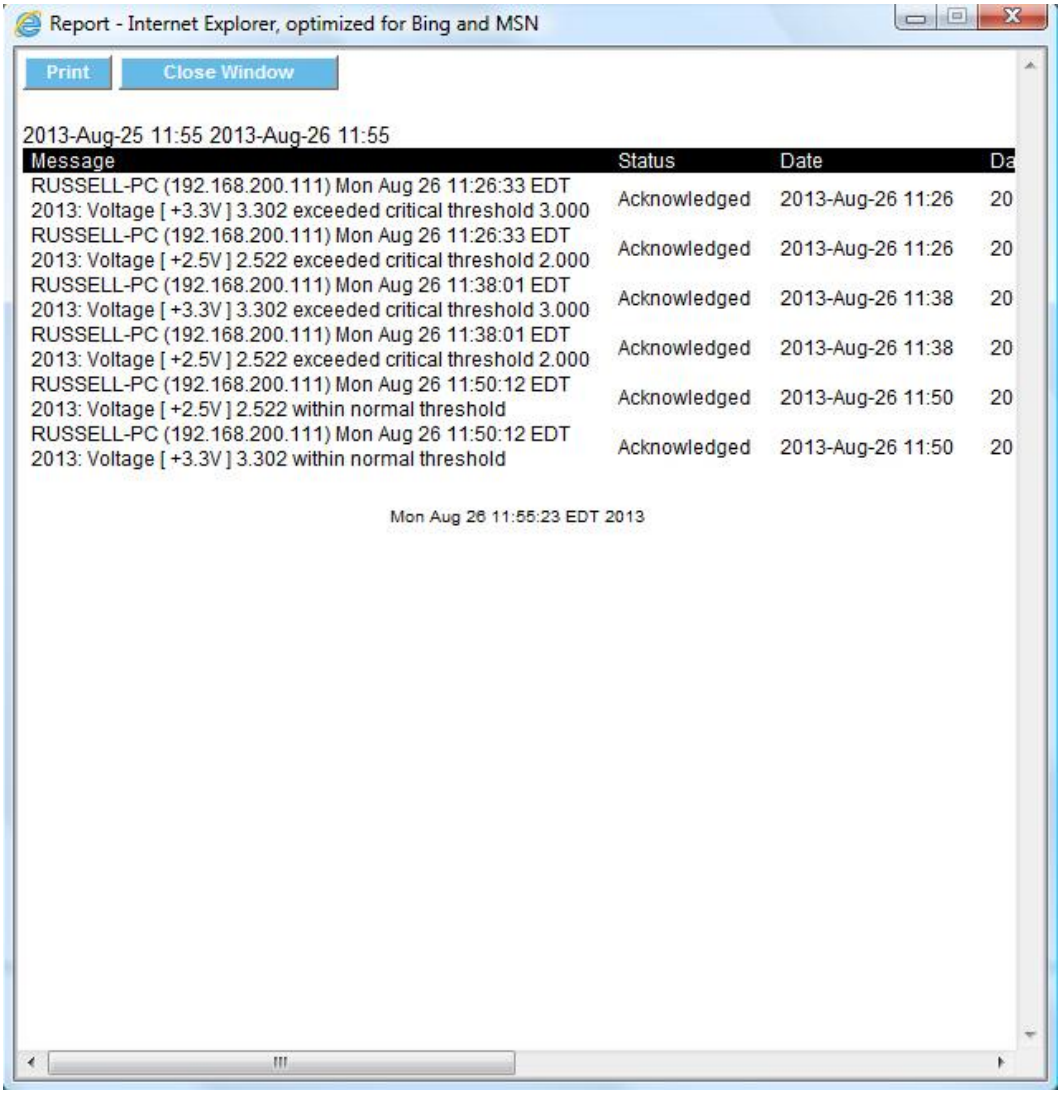
Report on a single machine by clicking the Single System radio button and entering an IP address. Report on all machines by clicking the Group radio button and the “Report on all systems” button. Report on selected machines by clicking the Group radio button and enabling Filter 1, and optionally, Filter 2.

Filter 1 options for this report:

- Asset Monitoring Events
- Hardware Events
- Storage Events
- Network Events
- Performance Utilization Events

Filter 2 options for this report:

- IP Address
- Machine Name
- User Name
- Domain


Report - Internet Explorer, optimized for Bing and MSN
Print
Close Window
2013-Aug-25 11:55 2013-Aug-26 11:55
Message
Status
Date
Da
RUSSELL-PC (192.168.200.111) Mon Aug 26 11:26:33 EDT 2013: Voltage [ +3.3V ] 3.302 exceeded critical threshold 3.000
Acknowledged
2013-Aug-26 11:26
20
RUSSELL-PC (192.168.200.111) Mon Aug 26 11:26:33 EDT 2013: Voltage [ +2.5V ] 2.522 exceeded critical threshold 2.000
Acknowledged
2013-Aug-26 11:26
20
RUSSELL-PC (192.168.200.111) Mon Aug 26 11:38:01 EDT 2013: Voltage [ +3.3V ] 3.302 exceeded critical threshold 3.000
Acknowledged
2013-Aug-26 11:38
20
RUSSELL-PC (192.168.200.111) Mon Aug 26 11:38:01 EDT 2013: Voltage [ +2.5V ] 2.522 exceeded critical threshold 2.000
Acknowledged
2013-Aug-26 11:38
20
RUSSELL-PC (192.168.200.111) Mon Aug 26 11:50:12 EDT 2013: Voltage [ +2.5V ] 2.522 within normal threshold
Acknowledged
2013-Aug-26 11:50
20
RUSSELL-PC (192.168.200.111) Mon Aug 26 11:50:12 EDT 2013: Voltage [ +3.3V ] 3.302 within normal threshold
Acknowledged
2013-Aug-26 11:50
20
Mon Aug 26 11:55:23 EDT 2013

# Application Utilization Report

The Application Utilization Report contains the following information:

- Application Name
- User Name
- Machine Name
- Minutes Run
- Frequency Of Use

The report can be sorted by Application Name, User Name, or Machine Name.

The administrator can hide the Application Utilization report so it is not displayed in the menu. In the folder `C:\SyAM\Jetty\syam\webapps\root\WEB-INF\` edit the file `syam.properties` setting the value `enable_app_util=false`. After editing the file, the SyAM System Area Manager Web Server service must be restarted.

Choose the time period to be covered by the report, either by clicking the radio button for the drop down menu and making a selection from the menu (Last 24 hours, Last 7 days, Last 30 days, All) or by clicking the radio button to specify From – To and entering dates.

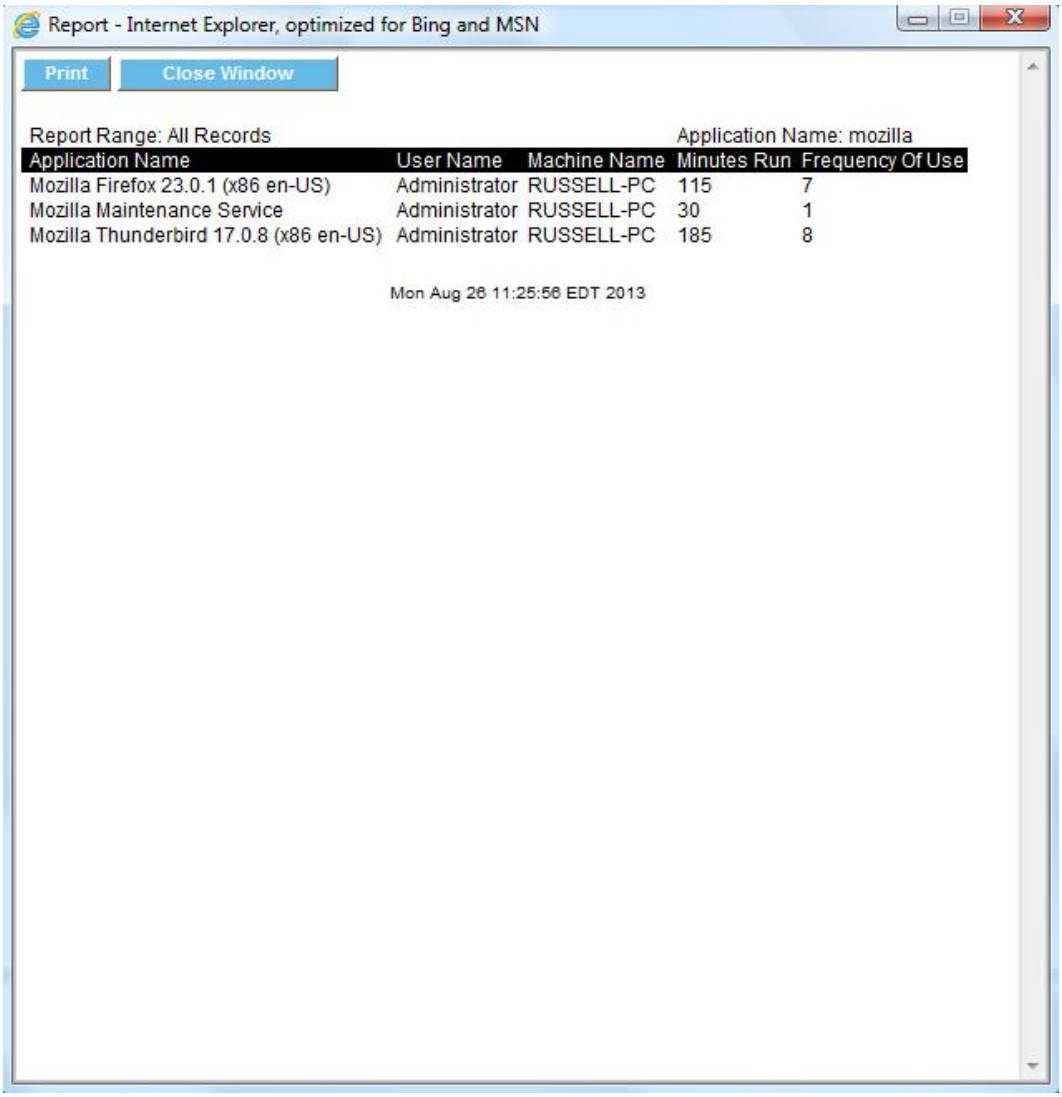
Enter the Application Name. The report will list all applications whose names contain the entered text. Report on all machines by clicking the “Report on all systems” button. Report on selected machines by clicking “Report on all systems that…” and enabling Filter 1, and optionally, Filter 2.

Filter 1 options for this report:

- Machine Name
- User Name
- Frequency
- Total Running Time

Filter 2 options for this report:

- Asset Number
- Board Model
- Function
- Health
- Installed Applications
- Location
- Logical Disk Free Space
- Machine Model
- Machine Name
- Operating System
- Owner
- Physical Disks
- Physical Memory
- Processor Model


Report - Internet Explorer, optimized for Bing and MSN
Print
Close Window
Report Range: All Records
Application Name: mozilla
Application Name | User Name | Machine Name | Minutes Run | Frequency Of Use
Mozilla Firefox 23.0.1 (x86 en-US) | Administrator | RUSSELL-PC | 115 | 7
Mozilla Maintenance Service | Administrator | RUSSELL-PC | 30 | 1
Mozilla Thunderbird 17.0.8 (x86 en-US) | Administrator | RUSSELL-PC | 185 | 8
Mon Aug 26 11:25:56 EDT 2013

# Power Hours Summary Report

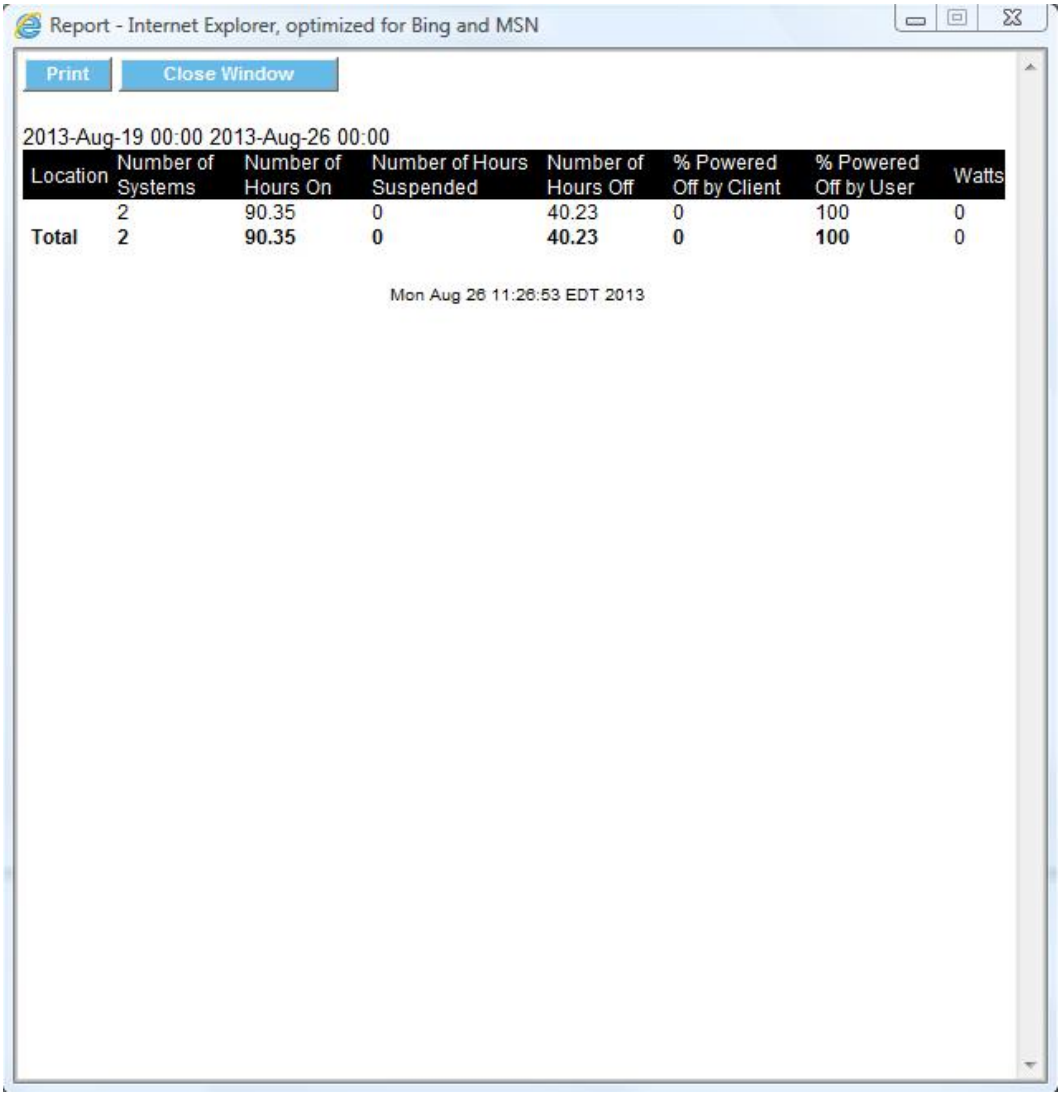
The Power Hours Summary Report contains the following information:

- Location
- Number of Systems
- Number of Hours On
- Number of Hours Suspended
- Number of Hours Off
- % Powered Off by Client
- % Powered Off by User
- Watts

Choose the time period to be covered by the report, either by clicking the radio button for the drop down menu and making a selection from the menu (Last 24 hours, Last 7 days, Last 30 days, All) or by clicking the radio button to specify From – To and entering dates.

Report on all machines by clicking the “Report on all systems” button. Report on selected machines by clicking “Report on all systems that…” and enabling Filter 1, and optionally, Filter 2.

Filter 1 and Filter 2 options for this report are the same as for the Application Summary Report.


Report - Internet Explorer, optimized for Bing and MSN
Print
Close Window
2013-Aug-19 00:00 2013-Aug-26 00:00
Location
Number of Systems
Number of Hours On
Number of Hours Suspended
Number of Hours Off
% Powered Off by Client
% Powered Off by User
Watts
2
90.35
0
40.23
0
100
0
Total
2
90.35
0
40.23
0
100
0
Mon Aug 26 11:26:53 EDT 2013

# Power Hours Detail Report

The Power Hours Detail Report contains the following information:

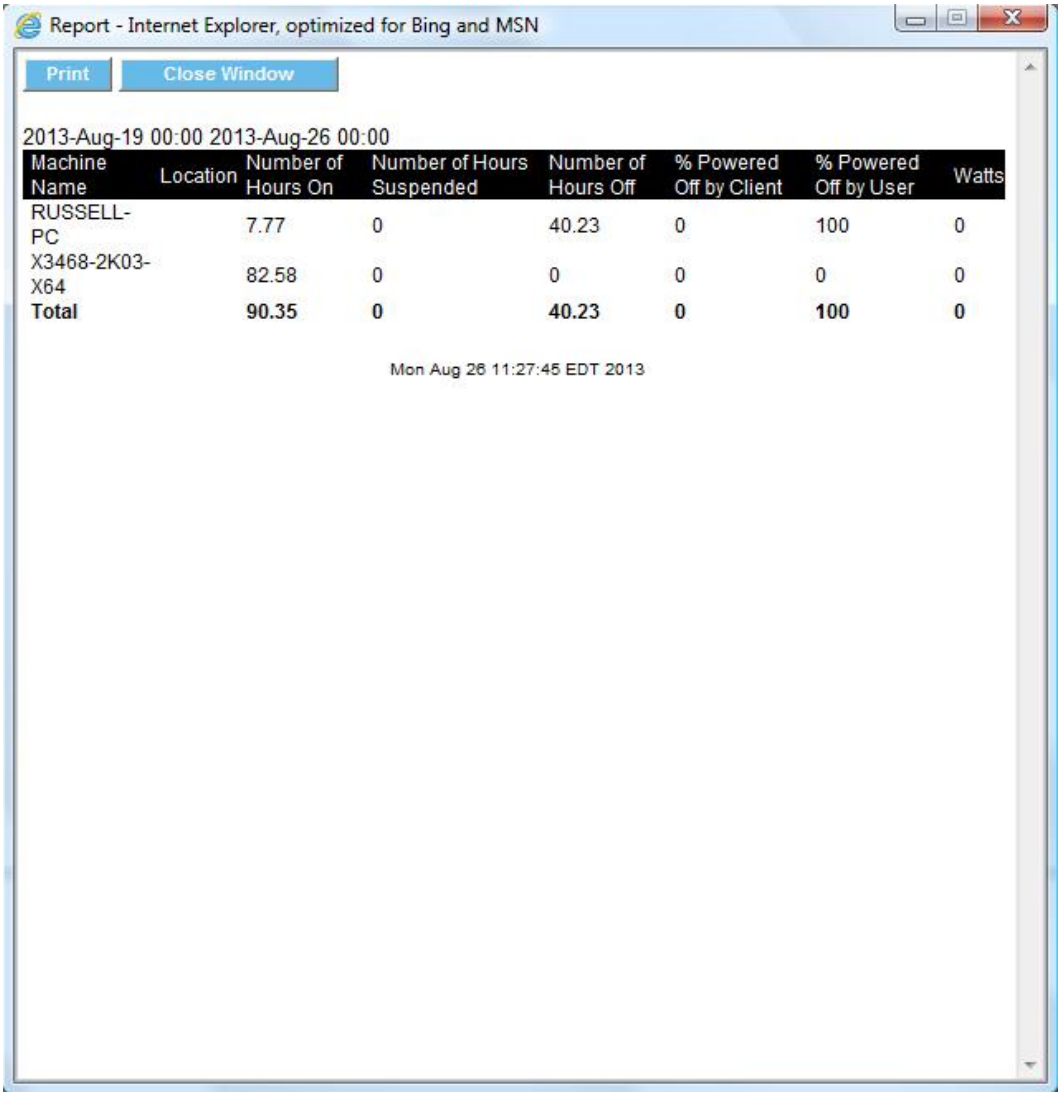
- Machine Name
- Location
- Number of Hours On
- Number of Hours Suspended
- Number of Hours Off
- % Powered Off by Client
- % Powered Off by User
- Watts

The Power Hours Detail Report includes information on individual systems, which is not included in the Power Hours Summary Report.

Choose the time period to be covered by the report, either by clicking the radio button for the drop down menu and making a selection from the menu (Last 24 hours, Last 7 days, Last 30 days, All) or by clicking the radio button to specify From – To and entering dates.

Report on all machines by clicking the “Report on all systems” button. Report on selected machines by clicking “Report on all systems that…” and enabling Filter 1, and optionally, Filter 2.

Filter 1 and Filter 2 options for this report are the same as for the Application Summary Report.

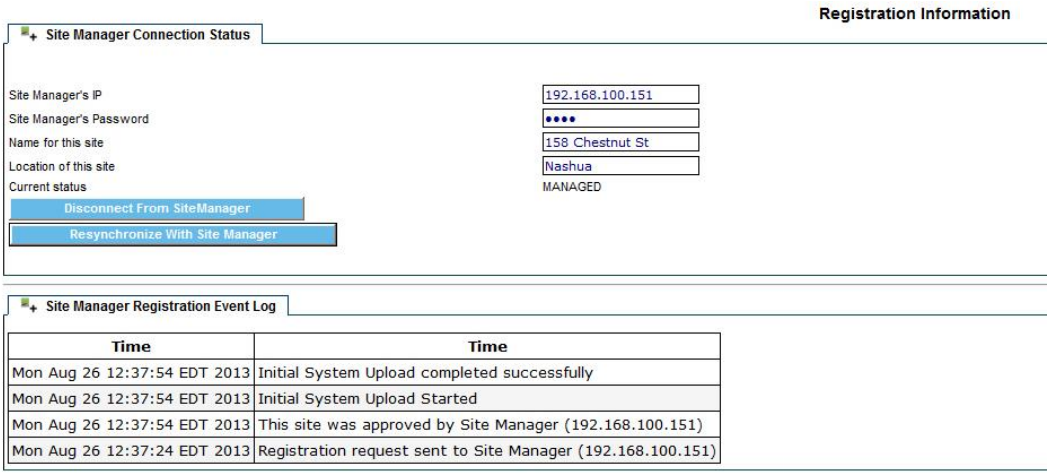

Report - Internet Explorer, optimized for Bing and MSN
Print
Close Window
2013-Aug-19 00:00 2013-Aug-26 00:00
Machine Name
Location
Number of Hours On
Number of Hours Suspended
Number of Hours Off
% Powered Off by Client
% Powered Off by User
Watts
RUSSELL-PC
7.77
0
40.23
0
100
0
X3468-2K03-X64
82.58
0
0
0
0
0
Total
90.35
0
40.23
0
100
0
Mon Aug 26 11:27:45 EDT 2013

# Chapter 8: Registering With Site Manager

The System Area Manager can be connected to the Site Manager. In order for the secure management communication to be enabled, you must register the System Area Manager to the Site Manager. To do this, choose Site Manager Registration from the drop down menu.

Enter the IP Address for Site Manager. The communication to Site Manager is encrypted TCP/IP so it can be over a WAN or the Internet. Now enter the Security password configured in Site Manager for System Area Manager communication. The Site Name and Location are the user defined fields that are used to identify the System Area Manager at the Site Manager.

Click the Register button and the System Area Manager will start the registration process.




Once the registration information has been successfully communicated to Site Manager it moves to status Pending Approval. The Site Manager must approve the System Area Manager before the status becomes Managed.

If you wish to stop the System Area Manager from reporting to Site Manager, click the Disconnect button. The System Area Manager can also be disconnected by the Site Manager.

All communication events are recorded and displayed below in the Site Manager Registration Event Log.

The default configuration of Site Manager allows System Area Manager to communicate with it using port 443. If you have configured Site Manager to use a different port for SSL, you will need to modify the System Area Manager configuration file **syam.properties** in this directory:
**C:\SyAM\Jetty\syam\webapps\root\WEB-INF**

Use a text editor to edit the file, changing this line:
`sitemanager_port=443`
to use the port used by Site Manager. After saving the file, restart the SyAM Software System Area Manager services.

# Chapter 9: Configuring System and Central Alerts

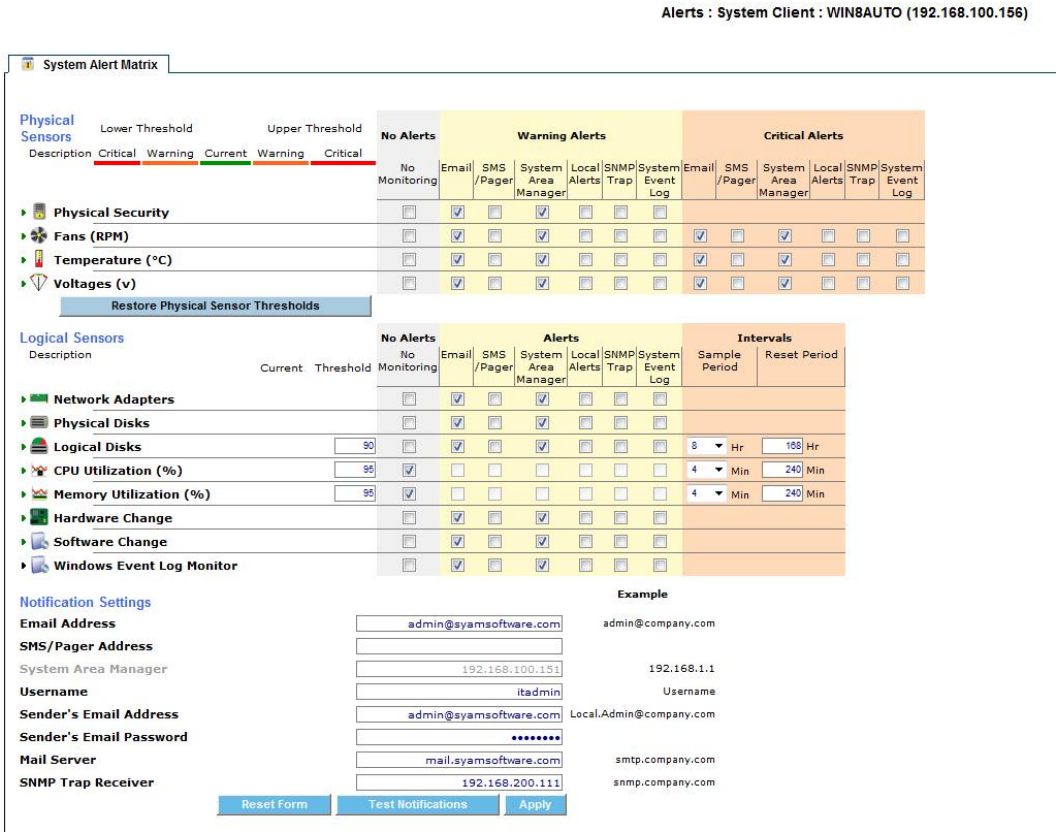
System Area Manager provides the ability to configure alerts at individual system and central levels.

By using the Area Manager, users may configure thresholds and sample/reset periods for each monitored resource. Several notification methods also become available, such as via SNMP Traps or Operating System Event Logs.

## System Alert Matrix – System Level Alerting

The System Alert Matrix provides a detailed, color-coded view of the status of all monitored components in a specific managed system.

Settings such as notification methods, thresholds, and sample periods for each sensor type category are automatically applied to all discovered sensor instances of that type.



# Monitored Sensor Types

## Physical Sensors

| | |
|---|---|
| | Security – If/when the system chassis is opened, the intrusion will trigger a sensor alert, provided that the connected board/BIOS support this information reporting. |
| | Fans – Monitored for rotational speed provided the fan is connected to a board/BIOS that supports the information reporting. |
| | Voltages – Monitored for the functionality that the connected board/BIOS supports. |
| | Temperature – Monitored for the functionality that the connected board/BIOS supports. |
| | Thermal Controlled Fans – Monitored for rotational speed and alerts when the CPU Temperature exceeds the defined threshold and the fan is not spinning. Provided for a defined set of motherboards supporting this feature. |
| | Wattage Utilization – Monitored for power consumption, provided that system hardware supports this information reporting. |
| | Redundant Power Loss – Monitors IPMI managed servers and alerts upon when redundant power systems lose their redundancy |

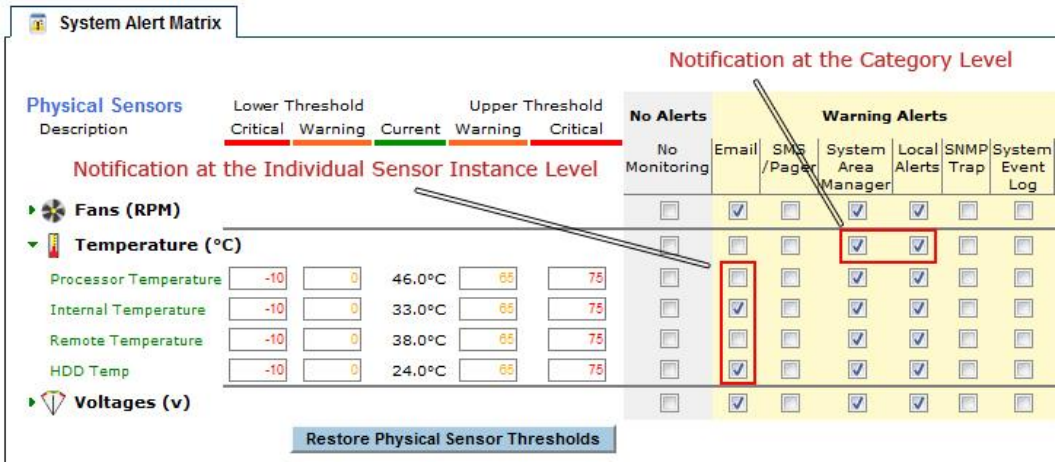
## Logical Sensors

| | |
|---|---|
| | Network Adapters – Monitors Ethernet operational state. |
| | Physical Disks – Monitors the presence and percent usage of a physical disk in the system and/or a RAID Set available to the operating system through a RAID controller. |
| | Logical Disks – The percent of capacity used by the logical disk formatted and mounted by the operating system is reported. If the disk has not been formatted, it will be reported as a failed disk.<br><br>Removable Device – Removable devices that are represented to the operating system will be reported as mounted as long as they are present in the system. |
| | Managed RAID Controller – RAID Controller health. |
| | Total CPU utilization – Percentage of CPU usage. |
| | Total Memory utilization – Percentage of Physical and Virtual Memory usage. |
| | Memory Error Rate – Number of Single- and Multi- Bit errors that have occurred (requires ECC memory and support by the server board) |
| | Hardware Change – Monitors changes to system hardware configuration. |
| | Software Change – Monitors changes to installed programs. |
| | Service Monitor – Monitors state of a system service. |
| | Process Monitor – Monitors state of a process. |
| | Windows Event Log Monitor – Monitors file size of a Windows event log. |

# Notification Settings

When a system is managed from the System Area Manager, it enables users to modify any of the thresholds, sample periods, reset periods, and notification methods. It also enables alerts to be sent via the other notification methods such as SMS/pager, Local Alerts, SyAM System Area Manager central alerting, SNMP Trap, or writing the event to the System Event Log.  (Note this System Event Log means events will be written to the local Windows Event Log or Linux syslog.)

Clicking on each sensor category tree expands it to reveal all instances in the category. To select an entire category of sensors for the alert, click on the bolded category header. To select individual instances, click on the appropriate boxes for each instance.




Each sensor category provides the default notification options, thresholds, sample periods and reset periods that will automatically be applied to newly discovered sensor instances within that category.

**Disabling Notifications**
If you wish to disable notifications for a specific senor or sensor category you can do this by clicking on the No Monitoring check box.

This disables the sensor instance or sensor category from having any alerts notified, thus they will not be monitored or be represented in the health state of that sensor category.

**Physical Sensor Upper and Lower Thresholds**
Each physical sensor instance has its own range of safe operating values with lower and upper warning and critical thresholds. These values are discovered if the hardware platform supports that information, or are calculated from available data.

**Physical Sensor Warning and Critical Alerts**
Since physical sensors may enter warning or critical health states, separate alerting methods may be configured for each.

**Logical Sensor Thresholds**
Monitored resources that are not physical sensors are called "Logical Sensors". Each instance of the logical sensor types Logical Disk, CPU Utilization, and Memory Utilization, has a utilization threshold.

**Logical Sensor Warning Alerts**
Logical sensors, by design, may enter the warning health state but not critical. So there is only a single set of alerting methods available.

**Sample Period**
CPU and Memory Utilization are gathered several times over a period of time, so that transient spikes are not reported. This time period is configurable by the administrator, and is known as the sample period. The pre-set sample period options are from 4-8 minutes. If 80% of the gathered readings exceed the threshold, a transition to warning state occurs.

The sample period for an instance of Logical Disk that is a removable device (floppy or CD-ROM drive) is similar to that of other sensors. A set of four readings is gathered during the sample period. If the device (floppy disk or CD) is present through all of them, a transition to warning state occurs.

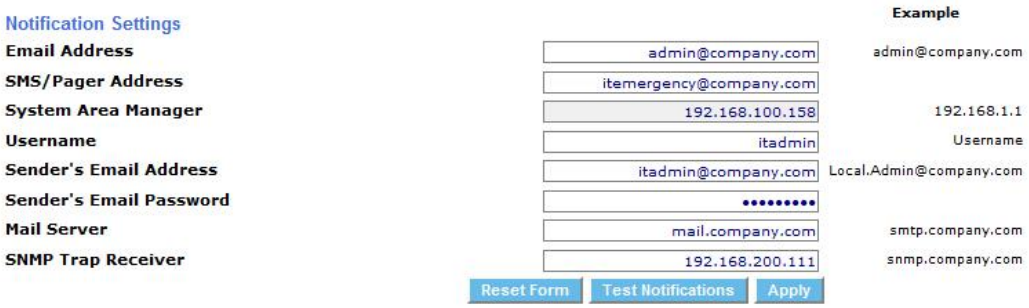
**Reset Period**
When a logical sensor transitions to a warning health state, an event is raised and alerts are sent according to the Warning Alerts settings. The reset period is the amount of time during which no additional alerts will be issued after the initial alert.

**Removing a Sensor Instance from the System Alert Matrix**
When a sensor instance, such as a specific logical or physical disk, has been removed from the system, or has otherwise entered a critical state, it is displayed in red and an "X" appears next to it. Click on the "X" to permanently delete this sensor instance from the alert matrix. Only do this if the instance is not being replaced. Once the sensor has been replaced it will automatically be monitored and the new health state will be represented.

**Hardware and Software Changes**
Alerts can be generated whenever the system hardware or software configuration is changed.

**Service, Process, and Event Log Monitors**
Monitoring of system services, processes, and Windows event log files can be configured on the system's Software tab.

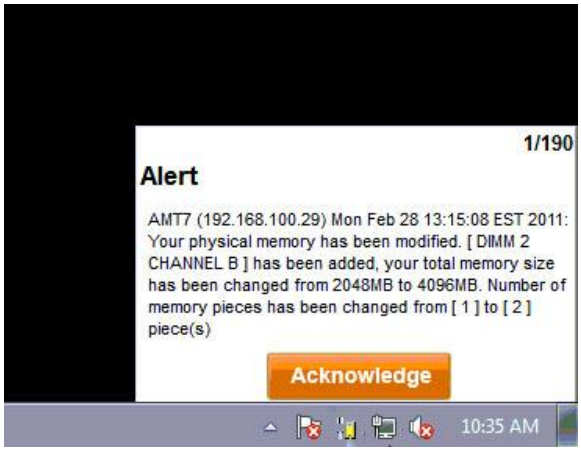
# Notification Settings – Configuring email alerting




Enter the destination email address, the sender's email address, and the mail server hostname or IP address. Enter the username and password if outgoing email is authenticated. Click the Apply button to save changes. Use the Test Notifications button to send a test email, and ensure your configuration is correct.

# Local Alerting

Enabling Local Alerts in the System Alert Matrix causes a tray icon to be displayed, and popup windows to appear, on the managed system when an alert is generated.




Alerts are categorized as asset monitoring events, hardware events, storage events, network events, and performance utilization events.

The user is prompted to acknowledge each alert. When the administrator generates a Local Alert report, each alert shows whether it has been acknowledged, and by which user.

# Central Alert Matrix

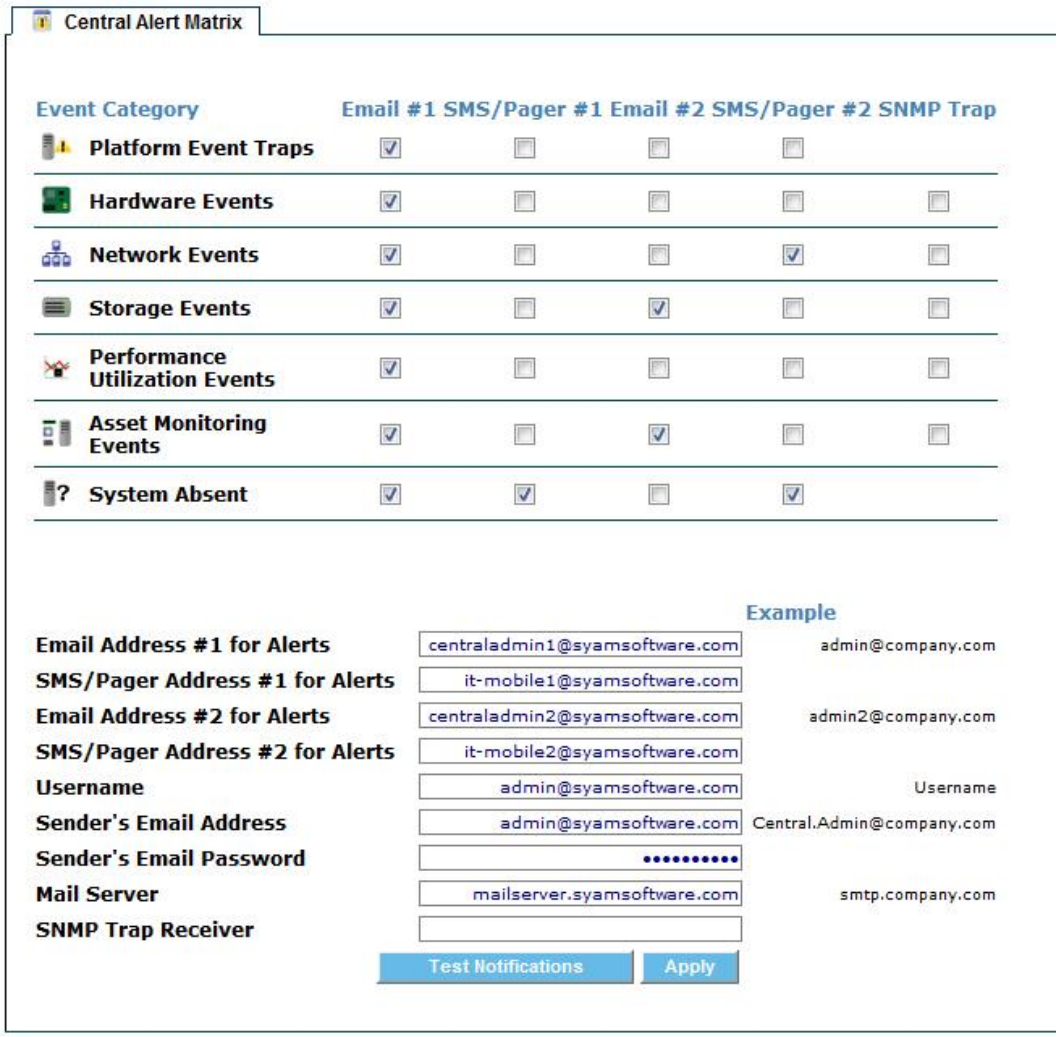
The Central Alert Matrix is accessed from the drop down menu on the header bar. It provides the ability to configure the appropriate notification options for events that are sent to this System Area Manager from all of the systems it is managing.

Notifications can be configured to be sent via email or SMS/Pager and can be assigned to administrator one or two for each type of event, in addition to sending SNMP Traps.

**Types of monitored events**

| | |
|---|---|
| | Platform Event Traps PET's – PET 1.0 formatted SNMP traps received are converted to plain text and alerted upon. |
| | Hardware Events – When a threshold is exceeded by a physical component within the system. Hardware Events include: physical chassis security, fan speed variation, chassis temperature fluctuation, voltage fluctuation or power redundancy loss |
| | Network Events – Network connectivity is lost due to an adapter failure. |
| | Storage Events – A logical disk has reached its utilization threshold, a logical or physical disk is lost (removed or not functioning), or a removable disk has remained present on the system for an extended period of time and may cause boot up issues. |
| | Performance Utilization Events – CPU or memory utilization threshold has been exceeded. |
| | Asset Monitoring Events – Server System Client records an inventory of the system components being monitored (i.e. CPUs, Memory, Disks, Software applications installed or removed, etc), and compares it each time the system is booted. Any discrepancy in the information when the agent is started is reported as an asset-monitoring event. |
| | System Absent Events – When the System Area Manager is no longer able to communicate with a managed system, it is reported as being absent, unless it was correctly shutdown. |

Central Alert Matrix can be configured based upon your notification requirements.




The Central Alert Matrix uses configurable SMTP email server settings. By default SMTP uses port 25 and does not use SSL. These settings can be modified as needed to support other SMTP email servers such as Gmail that uses SSL and port 465. To modify these settings, on the server running System Area Manager, stop the services SyAM Software System Area Manager Web Server and SyAM Software System Area Manager Central Manager. Edit the file syam.properties located in the c:\syam\jetty\syam\webapps\root\web-inf folder. When finished editing, restart the services.

**Default setting**
smtp_port=25
ssl=false

**Gmail setting**
smtp_port=465
smtp_ssl=true

**Not reporting IP Address in Alert Email**
You can modify alerting not to include the IP address in the alert email of the system by changing the value for notificationsDisplayIp from true to false.

# Integration into Enterprise Frameworks

## System Area Management (SyAM) MIB

The SyAM MIB must be installed into the Enterprise Framework server before it can decipher traps sent from a managed system.

Please consult your Enterprise Framework application on how to install a 3rd party MIB.

The MIB file is available for download from the SyAM website.

## System Area Management (SyAM) Integration into Microsoft System Center Operations Manager 2007/2012 (SCOM)

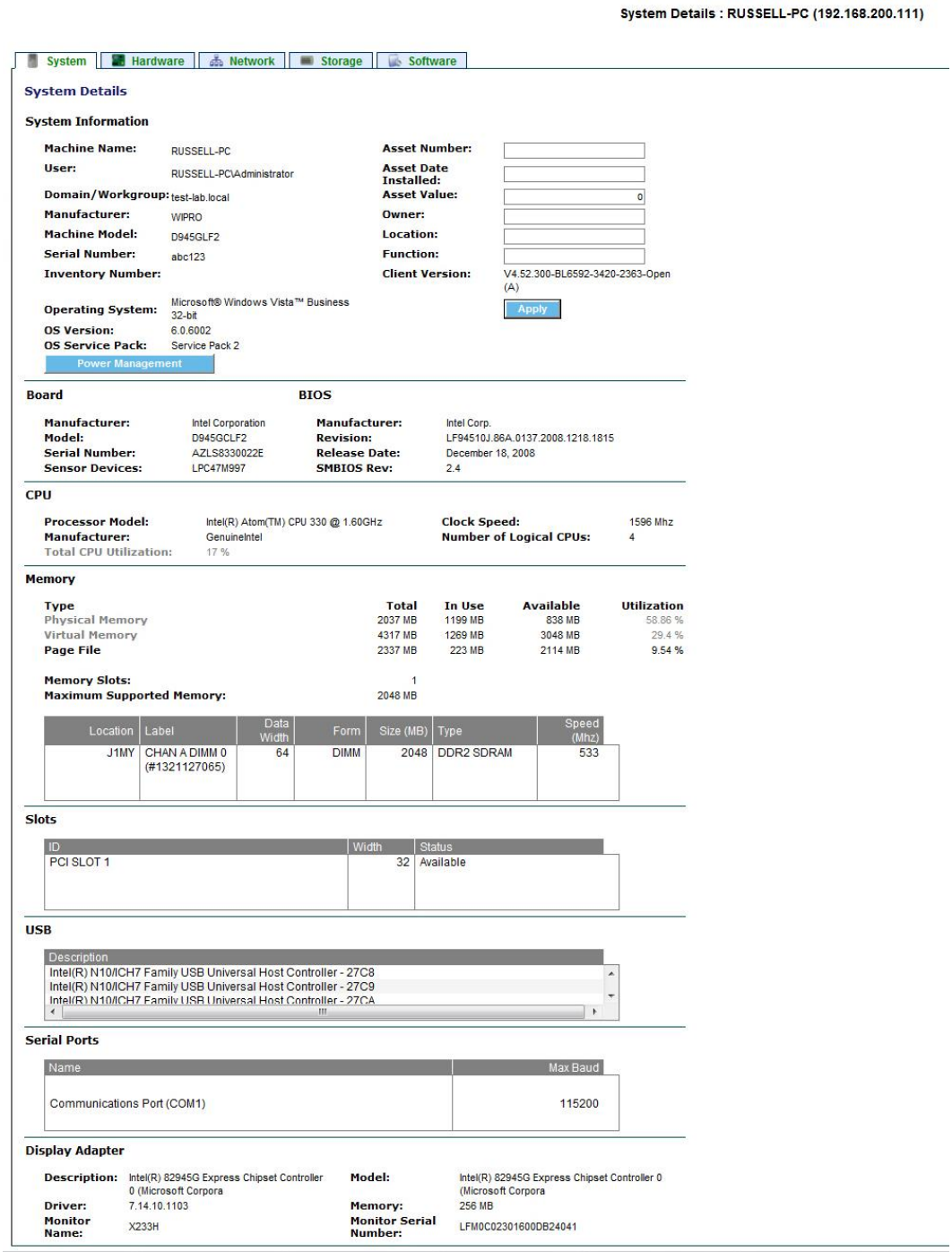
The SyAM Management Pack for Microsoft System Center Operations Manager must be imported into the SCOM server, before it can decipher Windows events written by SyAM Management Agents. Please consult the SyAM Software Tool Tip “Using the SyAM Events Management Pack” for instructions on installation and configuration.

The SCOM 2007/2012 Management Pack file is available for download from the SyAM website.

# Chapter 10: Accessing System Information

## System Detail Tab

The System Tab displays detailed information on the system’s configuration, including BIOS, vendor information, operating system, location, machine name, function, memory and CPU utilization, etc.  Administrators can choose to enter additional system information by filling in the fields at the top of the screen. The system's power management policies can be viewed and re-configured remotely by clicking on the Power Management button.



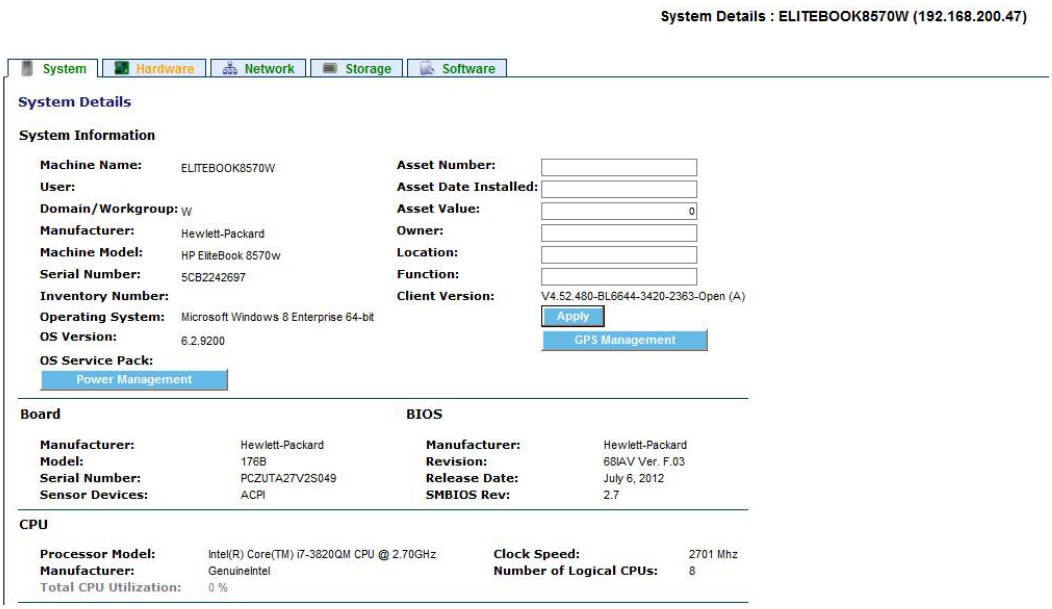

## Monitoring Memory Errors

***SyAM provides real time monitoring and alerting of single- and multi-bit memory errors on systems with supported ECC Memory error monitoring.***

The default alerting thresholds are to notify the administrator immediately on a multi-bit error or when two single-bit errors occur within a day. Through the SyAM System Area Manager Interface the administrator can adjust the thresholds and polling interval periods for both single- and multi-bit errors, and configure their notification methods.

## GPS Management

For supported systems with SyAM System Client 4.50 or newer, the GPS Management button is displayed.

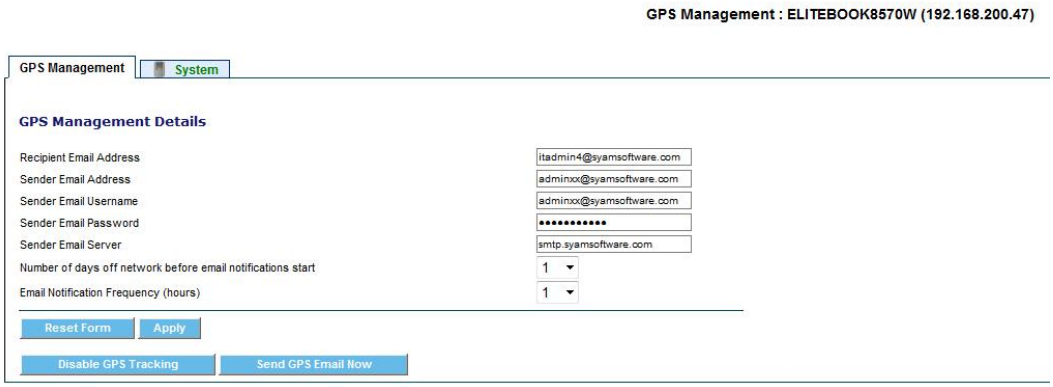



Enabling the GPS Management feature causes an email to be sent when a system has been off the network for a specified period of time. The email specifies the system's current location.

**Subject:**ELITEBOOK (192.168.10.34): GPS Email Notification
**Date:**Mon, 11 Mar 2013 15:15:02 -0400
**From:**audit@syamsoftware.com
**To:**audit@syamsoftware.com

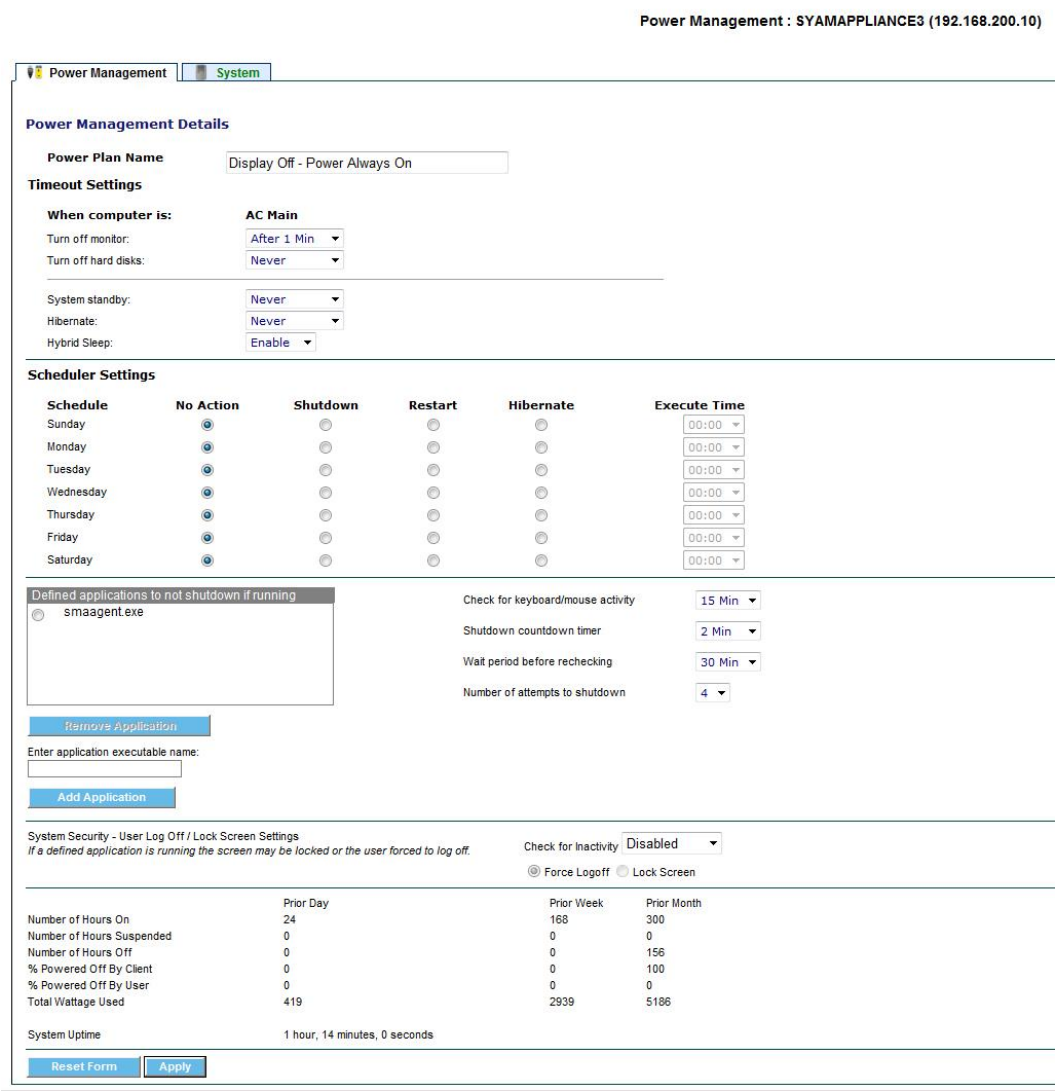
ELITEBOOK (192.168.10.34) Mon Mar 11 15:15:43 EDT 2013: GPS Email Notification
http://maps.googleapis.com/maps/api/staticmap?size=1024x768&maptype=roadmap&markers=color:red%7Clabel:I%7C42.8250673,-71.3677596&sensor=true
Time: Sat Mar 09 18:27:50 EST 2013
Latitude: 42.8250673000
Longitude: -71.3677596667
Altitude: 76.9470000000
Radius Error Margin: 250.0000000000
Altitude Error Margin: 13.0000000000
Tracking URL:
http://maps.googleapis.com/maps/api/staticmap?size=1024x768&maptype=roadmap&markers=color:red%7Clabel:A%7C42.8250673,-71.36775967&markers=color:red%7Clabel:B%7C42.82501345,-71.36769357&markers=color:red%7Clabel:C%7C42.82500655,-71.36768583&sensor=true
Tracking History:
A - Sat Mar 09 18:27:50 EST 2013
B - Sat Mar 09 18:28:50 EST 2013
C - Sat Mar 09 18:29:50 EST 2013

On the GPS Management page, configure email setting, specify the number of days (1 to 30) the machine must be off the network before notifications are sent, and the number of hours (1, 2, 6, 12, 24, or 48) between notifications.




# Power Management Tab

The Power Management tab lets the user display and reconfigure power management policies for the managed system.




**Power Plan Name**

The Power Plan Name for a newly installed SyAM Windows Client is the name of the active Windows Power Scheme. Setting up a new power plan here, or in the SyAM Management Utilities, will create a new Windows Power Scheme and make it the active power plan.

**Timeout Settings**

From here you can configure the power scheme settings for the managed system. If the managed system is a notebook or tablet there will be two separate sets of settings: one set that will be applied when connected to AC Power, and the other set for when running on battery.

The options are;

- Turn off monitor
- Turn off hard disks
- System standby
- Hibernate – This will only be displayed if the system has hibernation enabled
- Hybrid sleep (disable or enable)

**Battery**
This information is only displayed if the managed system is a notebook or tablet.

Current Power Source – States if the system is plugged in using AC Power Cord or is running from the battery
Battery Charging – States if the battery is in a charging state
Battery Level – Current health state of the battery
Battery Charge – The percentage of battery life available

**Scheduler Settings**
You can configure the managed system to be scheduled to perform a graceful system shutdown, restart or hibernation at any time for each day.

To enable, click on the appropriate radio button for the action to be taken that day. (No Action / Shutdown / Restart / Hibernate). Then set the time using the drop down box.

Different actions can be set at different times for each of the days of the week.

Only one action per day can be scheduled.

Press the Apply Button to save the changes made.

**Defined applications to not shutdown if running**
You can enter the name of an application if found to be running it will not perform the scheduled shutdown.

To add an application, Enter the name of the application executable and press the Add Application button.

To remove an application, click on the radio button next to the application you wish to remove and press the Remove Application button.

**Check for Keyboard/Mouse Activity**
This is the time period that is checked before attempting to perform a scheduled shutdown.

**Shutdown Countdown Timer**
This is the time period that the user is presented to cancel the scheduled shutdown.

**Wait Period before Rechecking**
This is the time period that the agent will wait before attempting to perform the scheduled shutdown.

**Number of Attempts to Shutdown**
This is the number of attempts the agent will attempt to perform the scheduled shutdown for that day.

**System Security – User Log Off/Lock Screen Settings**
This feature is used to secure a system against unauthorized access when the user is not present. Use the drop down menu to enable the feature and select the inactivity timeout period. Then choose either to force a logoff of the currently logged-in user, or lock the screen, requiring the user to re-enter a password.

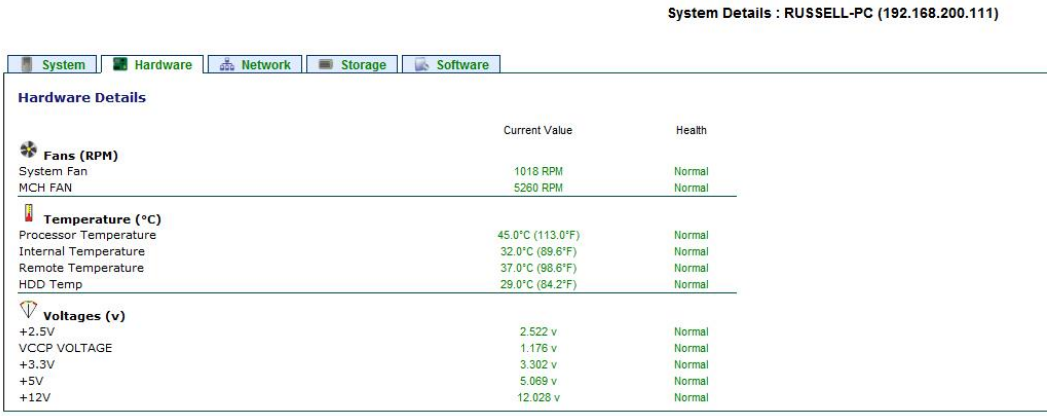
**Power Consumption**
Information on system power consumption is displayed here for the prior day, week and month.

Number of Hours On – total number of hours system is powered on
Number of Hours Suspended – total hours in suspended power state
Number of Hours Powered Off – total number of hours system is powered off
% Powered Off By Client – percentage of system shutdowns performed by the System Client
% Powered Off By User – percentage of system shutdowns performed by the user

**System Uptime**
How long the system has been running, as reported by the operating system.

# Hardware Detail Tab

All environmental sensors discovered on your platform are displayed in the Hardware Tab. This includes fans, temperatures, voltages, power redundancy loss and physical security. The number and type of sensors displayed is dependent upon the system platform and its configuration.

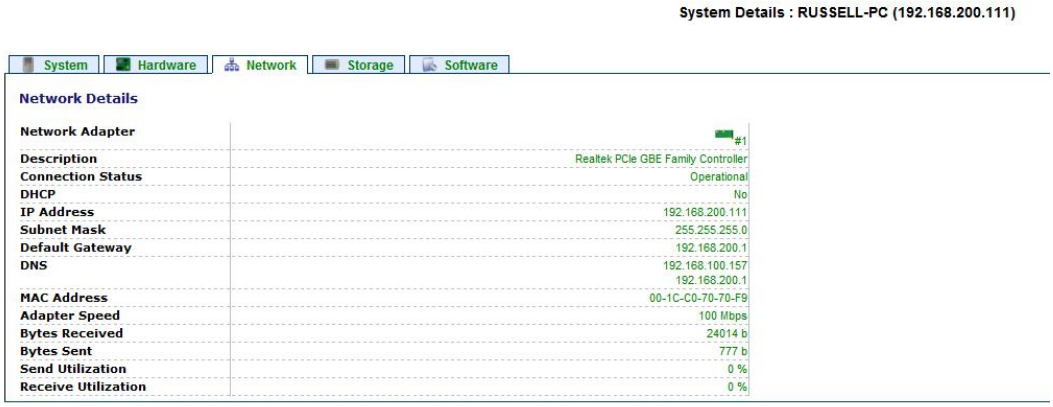



## Reset Chassis Intrusion

Some hardware platforms that support a chassis intrusion sensor, do not automatically reset the sensor state to normal when the chassis in closed.  For such systems the Reset Chassis button causes the platform to reset the state of the sensor to normal.

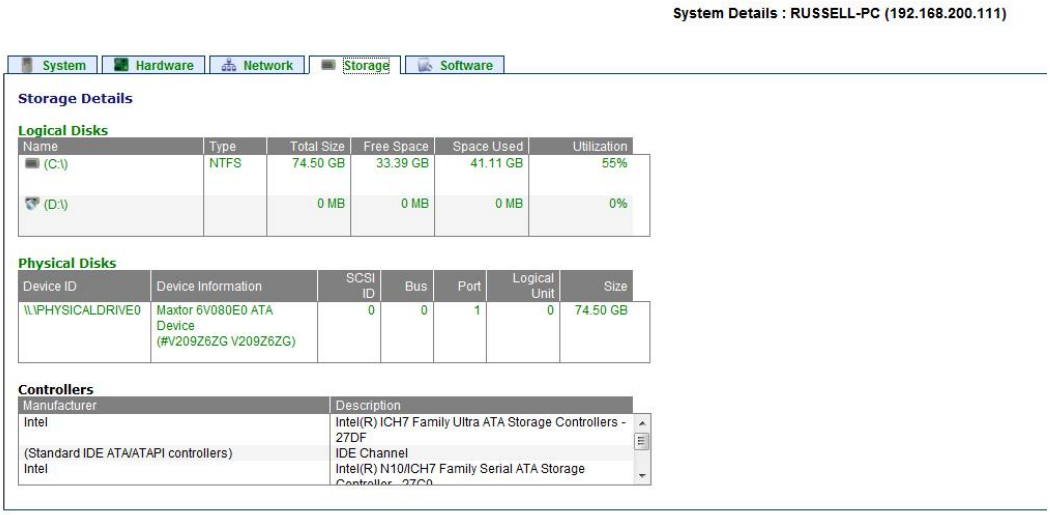
# Network Detail Tab

The Network Tab displays detailed information on adapters connecting the managed system to the network, including adapter and connection speed, connection status, IP address, and MAC address. Additionally the send and receive byte counts and calculated utilization over the last approximately 60 seconds is provided.



# Storage Detail Tab

The Storage Tab displays detailed information on physical and logical disks associated with the system being monitored. Physical disk attributes reported include vendor information, device ID, SCSI ID, and size. Logical disk attributes reported include name, size, space allocation, and utilization.




## SMART Drive Pre-Failure Monitoring

Directly attached disk drives that are SMART capable are checked daily. Supported disk technologies include P-ATA, S-ATA, SCSI and FC. The administrator can be notified of bad disk drives before they fail and potentially lose data. Notification of a bad SMART status (Pending failure) is done via the notification options configured for the drive.

The Storage Details tab visually shows physical drive status. A physical drive in the warning state (amber colored) is pending failure and has reported a bad SMART status.

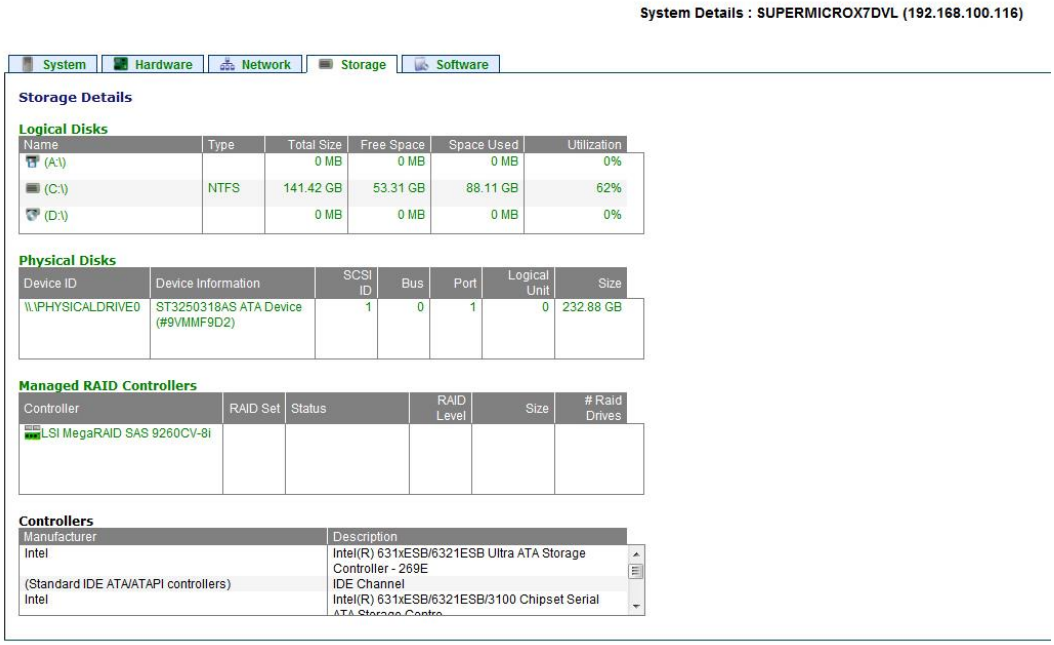
## RAID Management

SyAM System Client – Server and Desktop performs integrated monitoring of PCI RAID Controllers. All discovered PCI RAID Controllers that we support will be monitored, and their summary configuration and status displayed under "Managed RAID Controllers" within the Storage tab.

SyAM System Client – Server and Desktop will discover RAID Controllers that it can manage only if the required RAID drivers are installed. If a new RAID Controller is installed after SyAM System Client – Server and Desktop has been started, then restart the system for it to discover the new Managed RAID Controller.

**Please check the release Notes for the list of RAID Controller compatibility for the version of software you are using.**

Managed PCI RAID controllers can be configured with SyAM System Area Manager - Server. Navigation begins from the Storage Details tab.




Click on the RAID Controller to open up the RAID Controller window.

## RAID Controller Details Screen

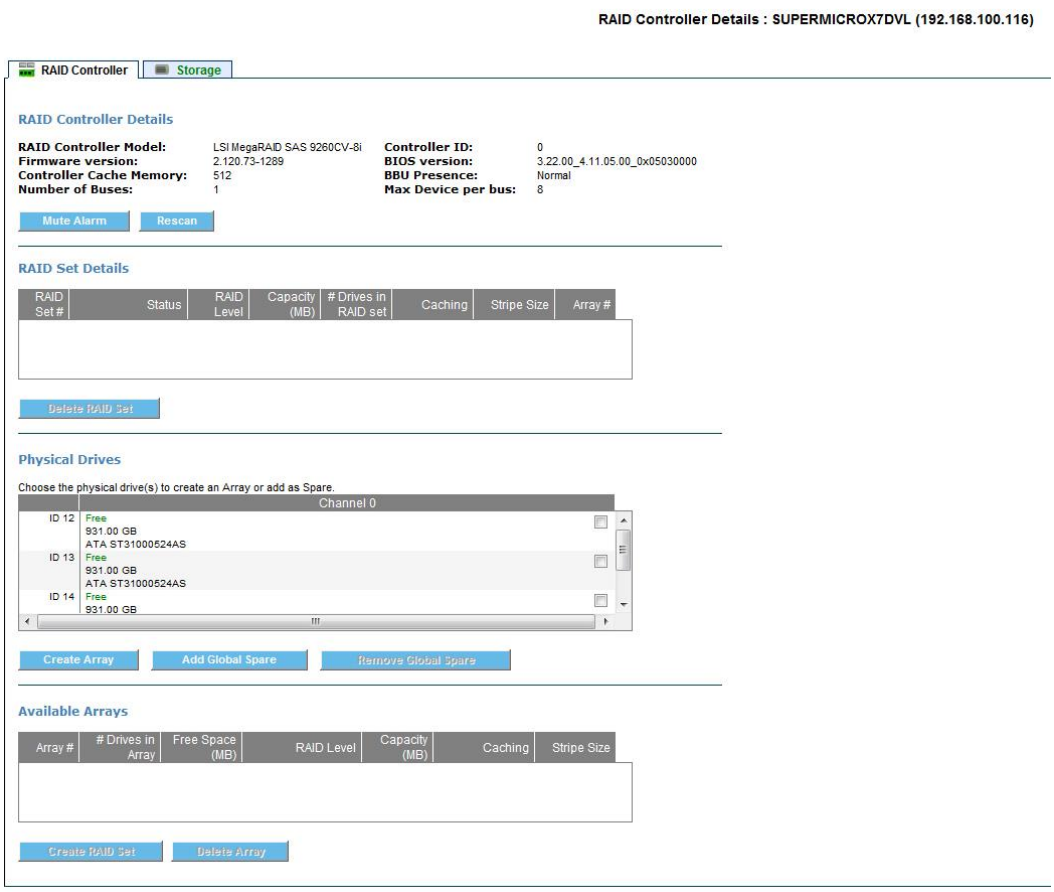
The RAID Controller screen is divided into 4 parts.

**RAID Controller Details** – Displays the controller model, firmware version, Cache if present, Number of Bus, ID, BIOS Version, BBU Presence and Max Devices per Buses

**RAID Set Details -** Displays the current RAID sets configured on this controller, including their description, RAID Set #, and Status (Normal, Init, Rebuild, Degraded, Failed). A RAID Set (also called a RAID Array) appears to the operating system as a physical disk.

**Physical Drives** – Displays the physical drives connected to the RAID controller, including their location on the BUS, ID, Status, Capacity, Vendor and Model. Physical drives in use by a RAID controller are typically not visible to the operating system.

**Available Arrays** – Displays the physical arrays defined by the RAID controller. A physical array is a grouping of drives on which RAID Sets are created. The display includes the RAID levels and capacities available for creating additional RAID sets.



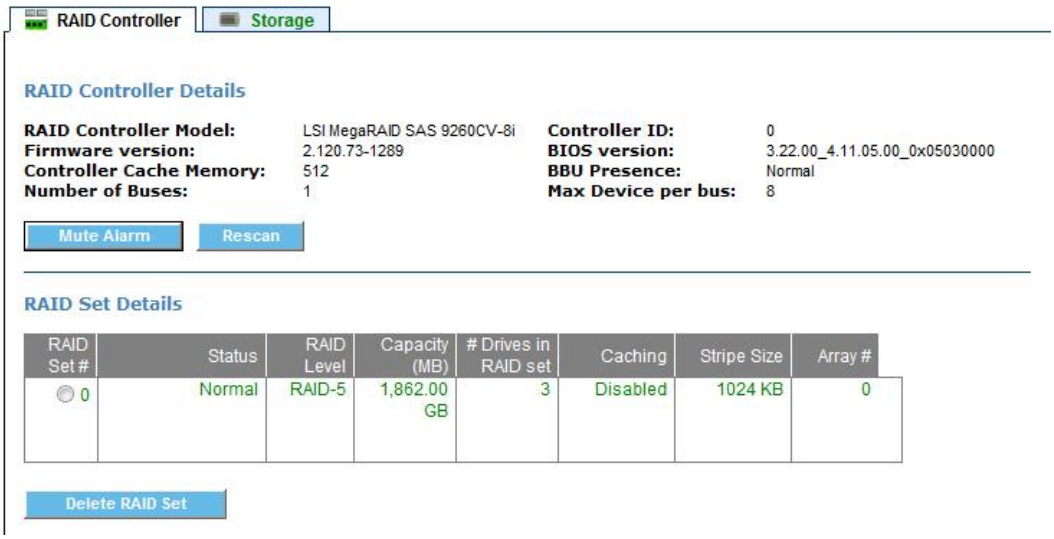

## Steps in Creating a RAID Set

1. Decide if you will create a RAID Set on an existing Physical Array, or want to first create a new Physical Array for the RAID Set. If you will use an existing Physical Array proceed to step 4.
2. To create a Physical Array, choose the physical drives that you wish to make up the array by clicking on their check box. (Remember only drives not in use in other arrays or as hot spares can be used.)
3. Click on the Create Array button – wait for the screen to update

4. Now click on the Physical Array that you wish to create the RAID Set on. (Physical Arrays **with no available capacity** will not display any available RAID Set configurations.)

5. Choose the RAID level from the drop down box. Only RAID levels supported for the particular set of drives in the Physical Array will be presented. The maximum capacity available for the selected RAID level is calculated and displayed. You may enter a lower capacity to be used for this RAID Set.

6. Next choose the Caching policy and stripe size from the drop down boxes.
7. Click the Create RAID Set button to create the RAID Set.
8. The system will now process your configuration and will create the RAID Set. If for any reason the create operation fails, a message will be displayed at the top of the screen explaining the cause for failure.
9. The new RAID Set will now appear under the RAID Set Details
10. If you created a Physical Array in Step 3 and decided not to create a RAID Set on it, you may dismiss it by selecting it and clicking the Delete Array button. You cannot delete Physical Arrays that have RAID Sets created on them.

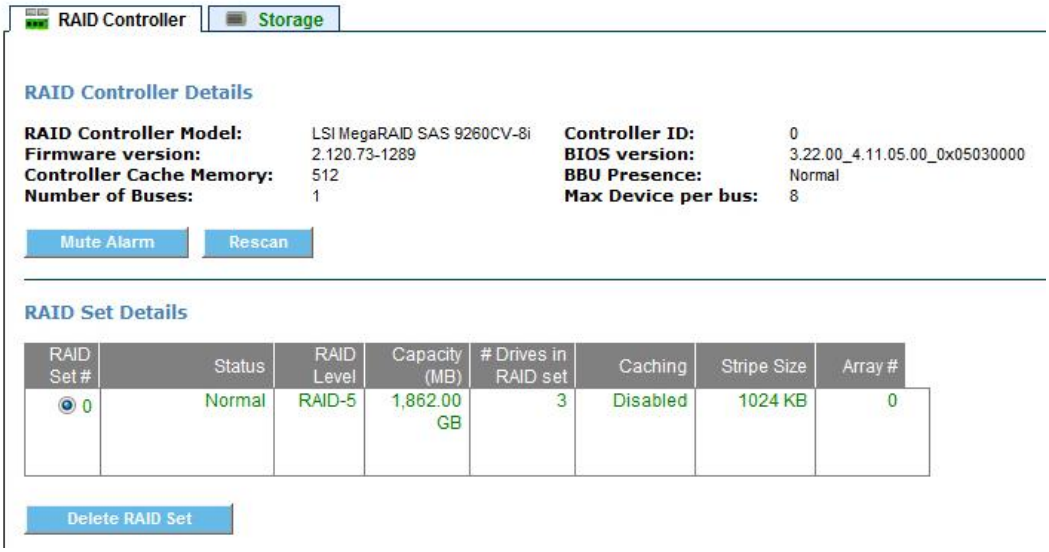


## Adding/Removing a Global Spare

1. Choose the physical drive that you wish to become a global spare to the RAID Set by clicking on its check box, then click on the Add Global Spare button.
2. To remove a global spare click on the check box next to the drive that is currently displayed as a hot spare, then click the Remove Global Spare button.

## Deleting a RAID Set

1. Under RAID Set Details click the radio button next to the RAID Set to delete. Then click the Delete RAID Set button. Note that when multiple RAID Sets are present on the same Physical Array, only the last RAID Set displays a radio button and may be selected to delete.



## SNMP Alerts for External Storage Devices

The System Area Manager can receive events from Infortrend and Dot Hill external storage devices when SNMP alerts are configured on the storage device and the SNMP trap receiver is configured for the IP address of the System Area Manager system.

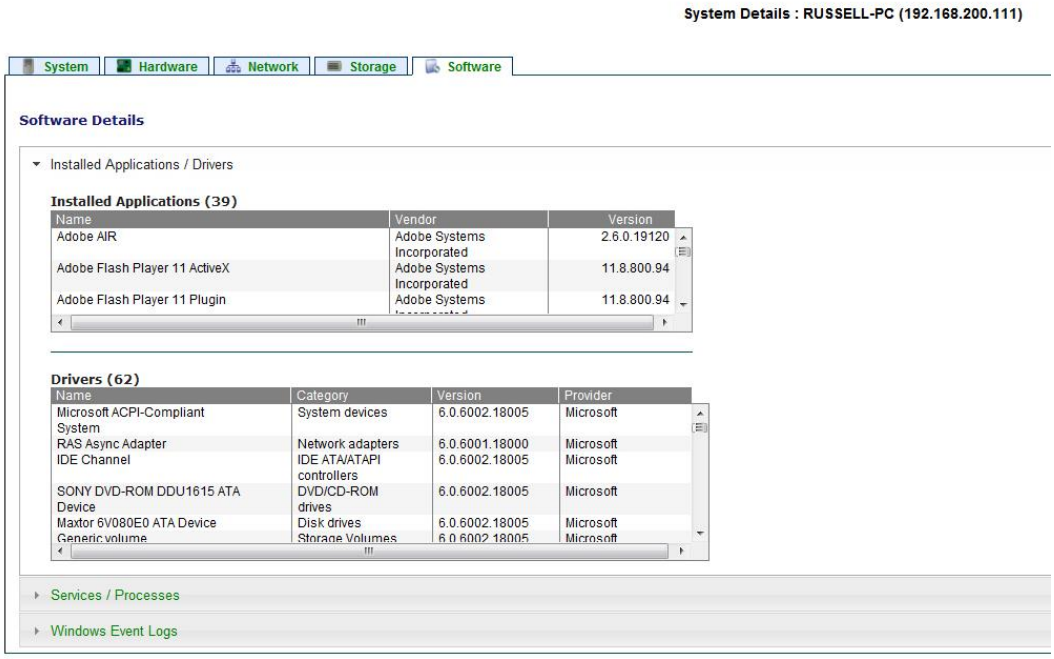
The System Area Manager will write the event messages to the Windows Application Event Log and the Area Manager Event Log, and can also be configured to send email alerts for the events received. An email alert will be sent if the Platform Event Trap check box is set and the email information is configured.

# Software Details Tab

The Software tab displays detailed information on the processes, services, applications and drivers installed and running on the system being monitored.

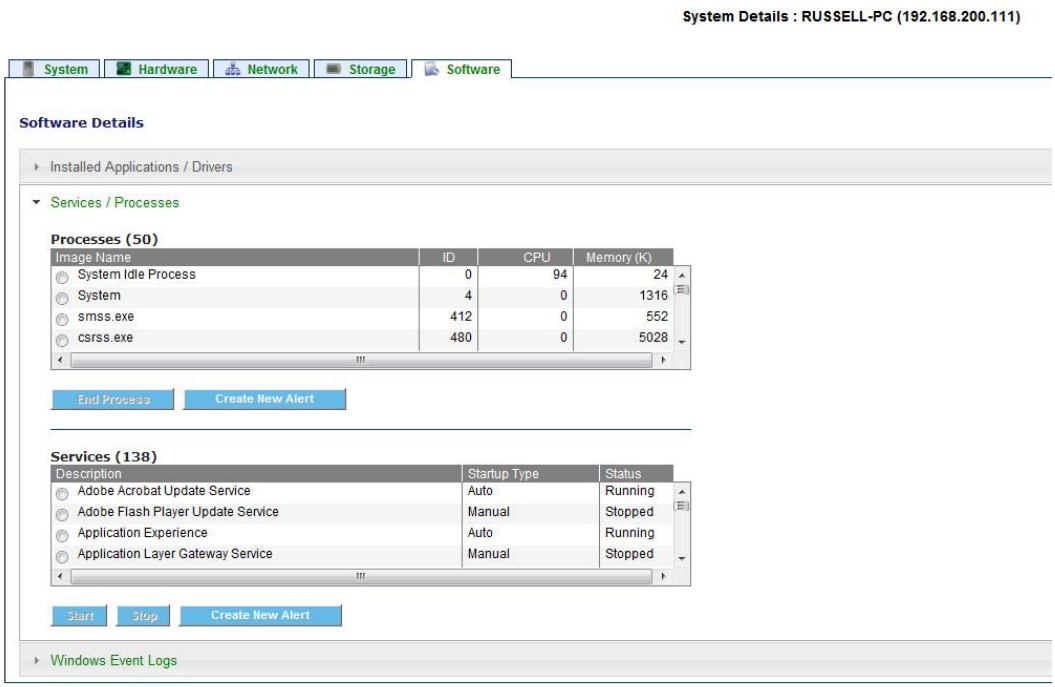
## Installed Applications and Drivers

Installed applications are listed with name, vendor and version information. The list of drivers includes name, category, version and provider.



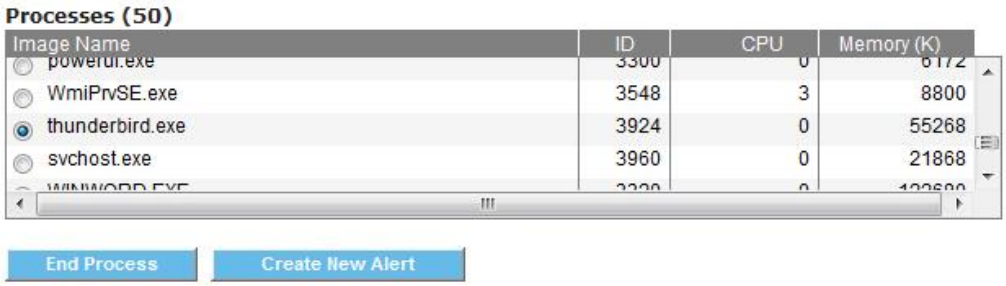

## Processes and Services

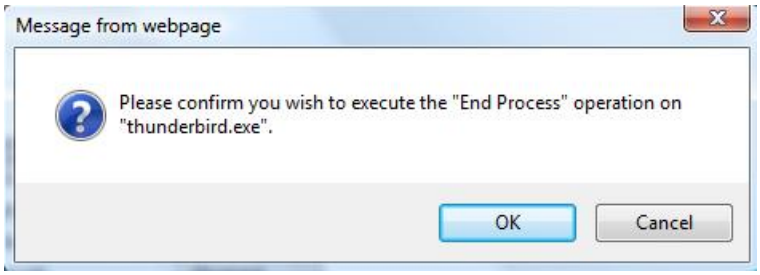
The list of running processes includes the process name, process ID, and CPU and memory utilization. The list of services includes description, startup type, and current state.



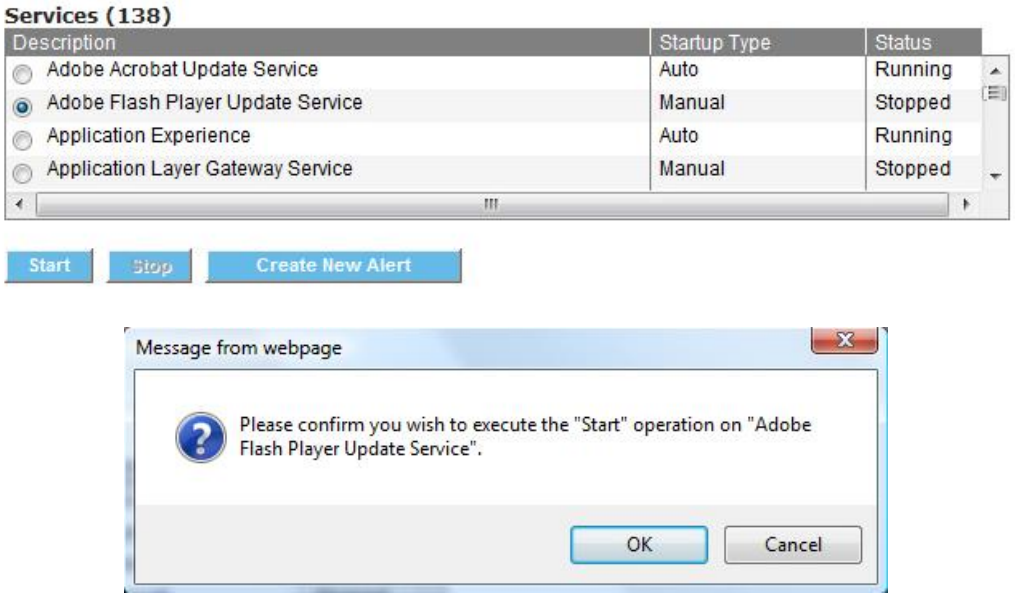

System Area Manager can stop a running process, and start or stop a service, on a managed system remotely through the browser interface.

To end a process, select the process by clicking the radio button to the left of the Image Name, then click the End Process button.

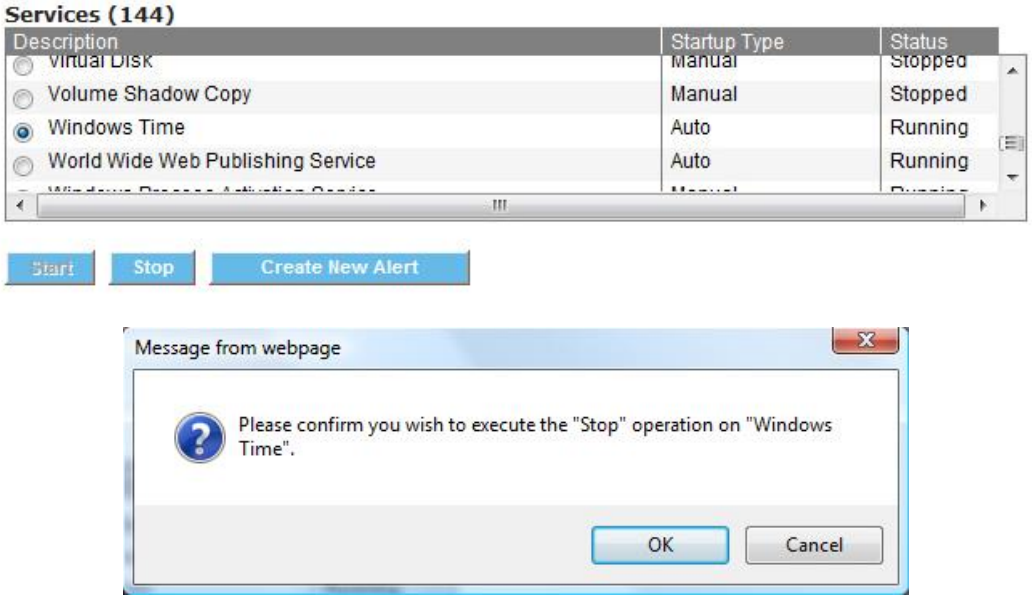


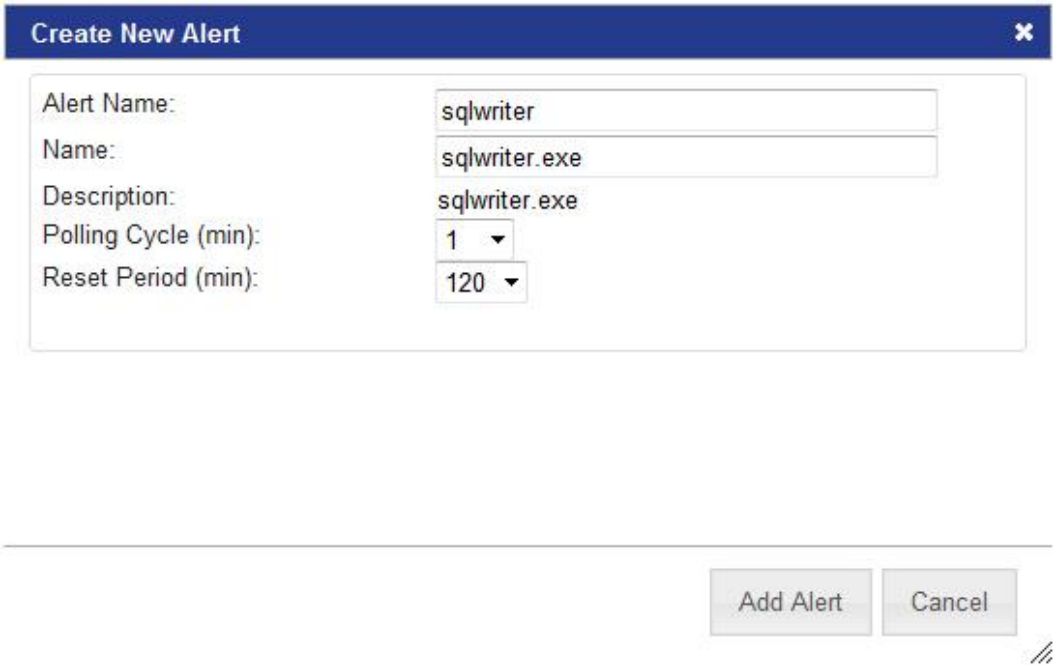

To start a service, select the service by clicking the radio button to the left of the Description (service name), then click the Start button. The service status must be Stopped in order to be started.




To stop a service, select the service by clicking the radio button to the left of the Description (service name), then click the Stop button. The service status must be Running in order to be stopped.



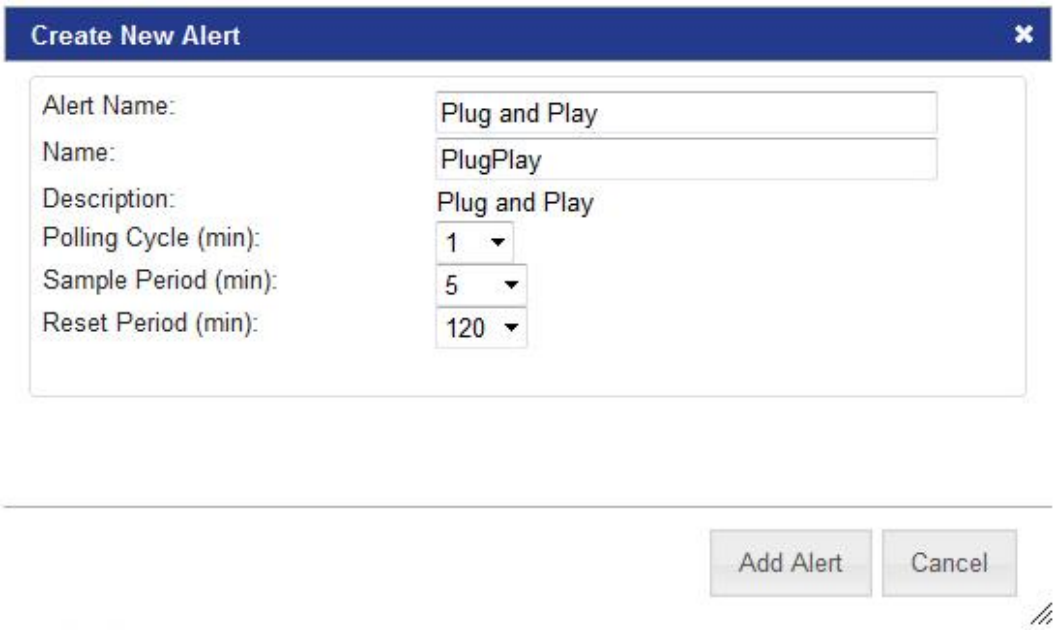

To create an alert on the status of a process, select the process by clicking the radio button to the left of its name, then click Create New Alert.




Enter an Alert Name. The alert will be listed by this name in the Software area and in the System Alert Matrix. The Polling Cycle controls how often the System Client will poll for process status. After an alert is generated, System Area Manager waits for the length of the Reset Period before sending another alert.

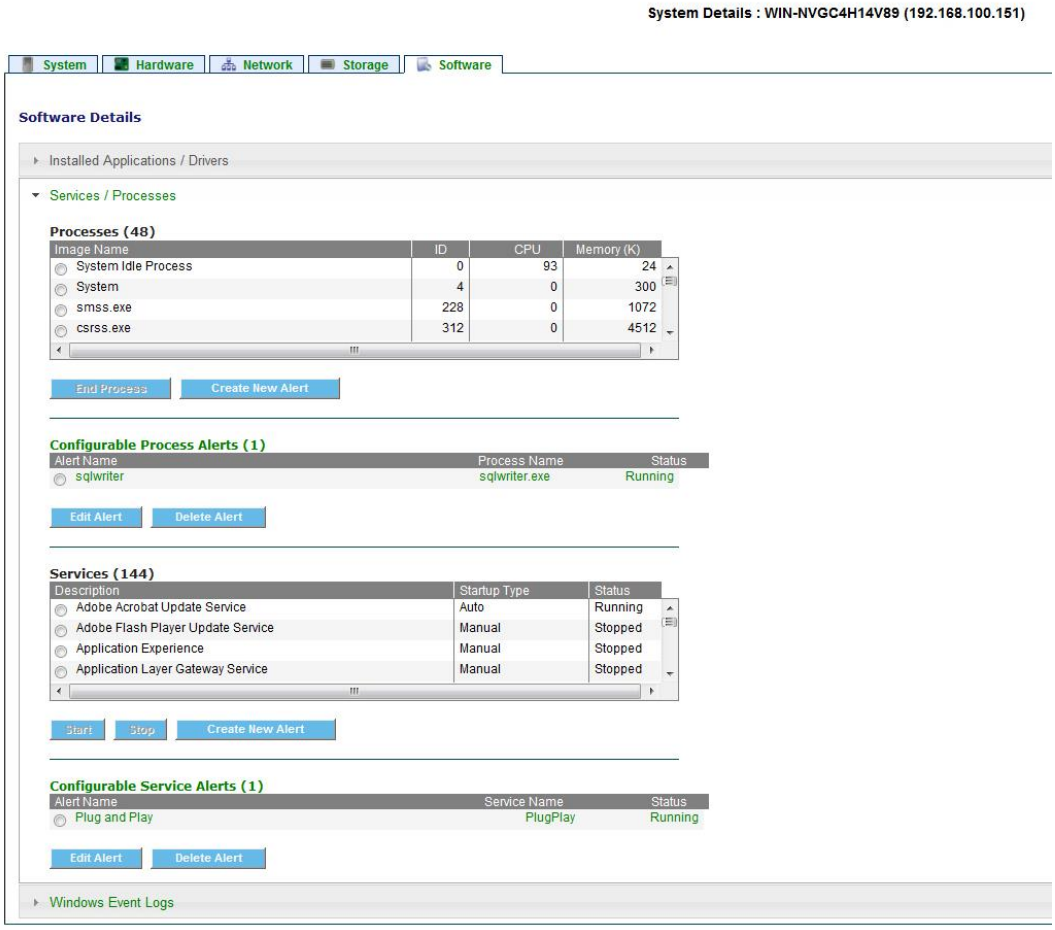
A system service alert will attempt to restart the service if it is not running. If the service is found to be not running for a second time during the Reset Period, an alert will be generated.

System service alerts are created in the same way as process alerts. Click the radio button to the left of the service name, then click Create New Alert.



Alert Name, Polling Cycle and Reset Period are the same for services as for processes. Service alerts also include the Sample Period, which is the number of minutes System Area Manager will wait to send an alert in order to give the service sufficient time to start.

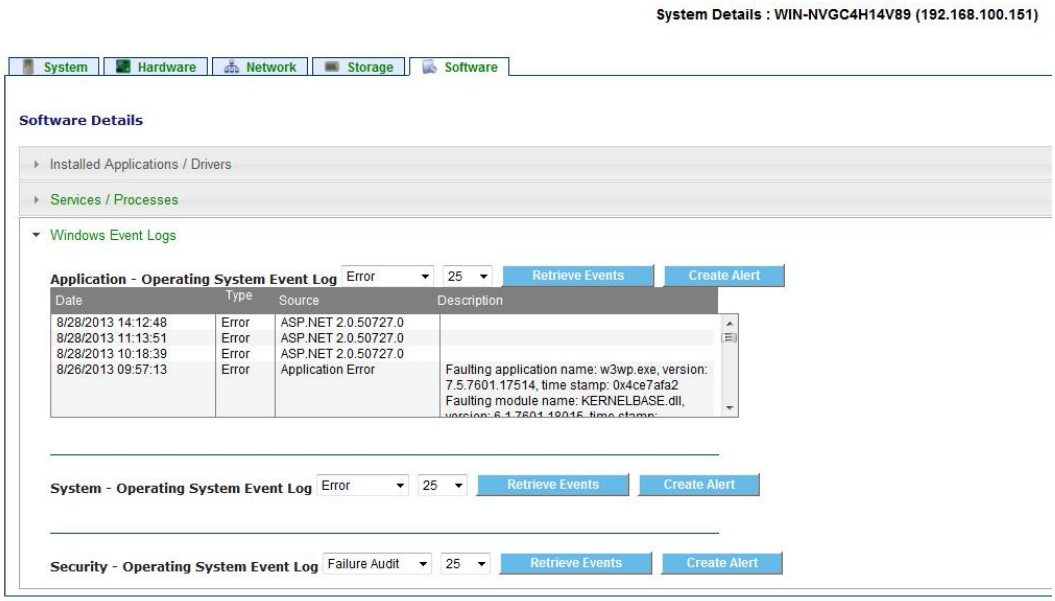
Once they have been created, configurable process and service alerts will be listed in the interface, where they can be edited or deleted.



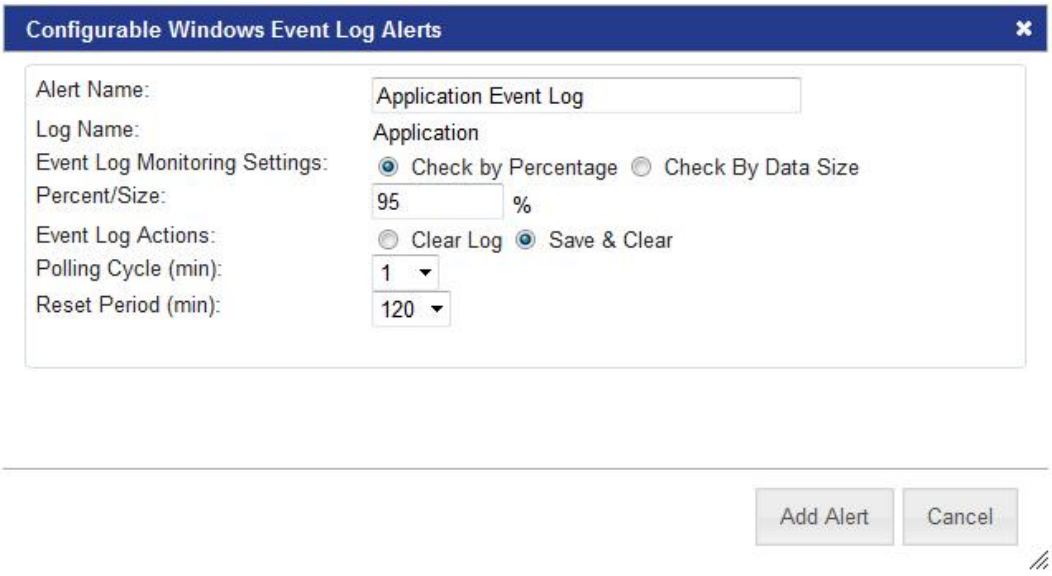

## Windows Event Logs

System Area Manager can retrieve events from Windows event logs, and can generate alerts when log files are cleared on reaching their size limits.

To retrieve events from the Application, System or Security event logs, first choose the event type to filter by. For Application and System logs, available event types are Error, Warning, and Information; for the Security event log, the options are Failure Audit and Success Audit. Next, choose the maximum number of events to be returned, up to 100. Click the Retrieve Events button.

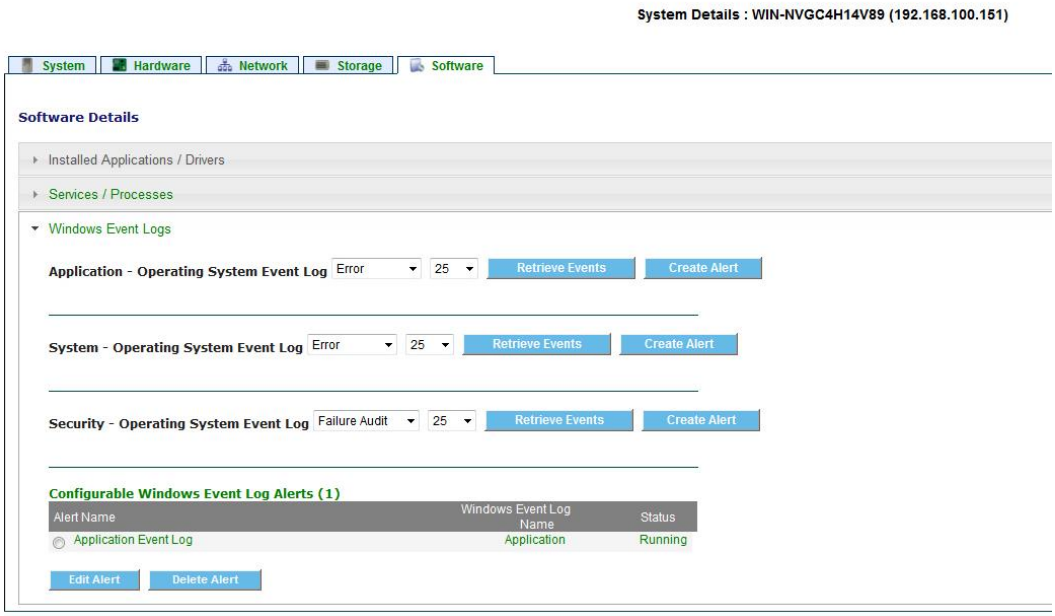



To create an event log alert, click the Create Alert button for the Application, System, or Security log.



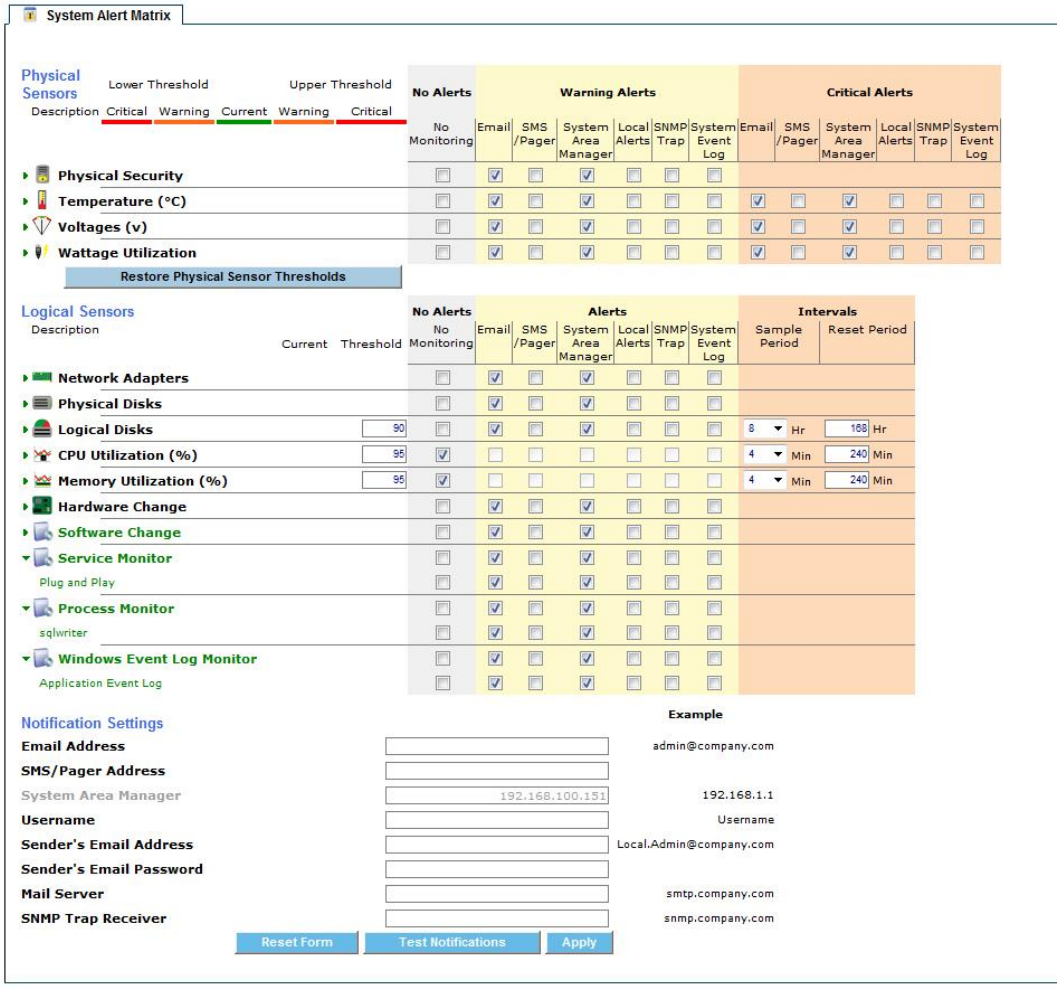

Enter a percentage of the maximum log file size determined by the operating system, or a size in megabytes. If the Save & Clear option is selected, the log file will be backed up in the same folder as other event files before the log is cleared. Older backup files will be overwritten.

Once they have been created, configurable event log alerts will be listed in the interface, where they can be edited or deleted.


System Details : WIN-NVGC4H14V89 (192.168.100.151)
System
Hardware
Network
Storage
Software
Software Details
Installed Applications / Drivers
Services / Processes
Windows Event Logs
Application - Operating System Event Log
Error
25
Retrieve Events
Create Alert
System - Operating System Event Log
Error
25
Retrieve Events
Create Alert
Security - Operating System Event Log
Failure Audit
25
Retrieve Events
Create Alert
Configurable Windows Event Log Alerts (1)
Alert Name
Windows Event Log Name
Status
Application Event Log
Application
Running
Edit Alert
Delete Alert

## Process, Service and Event Log Alerts

Alerts created in the Software section will be listed in the System Alert Matrix, where alerting options can be configured.

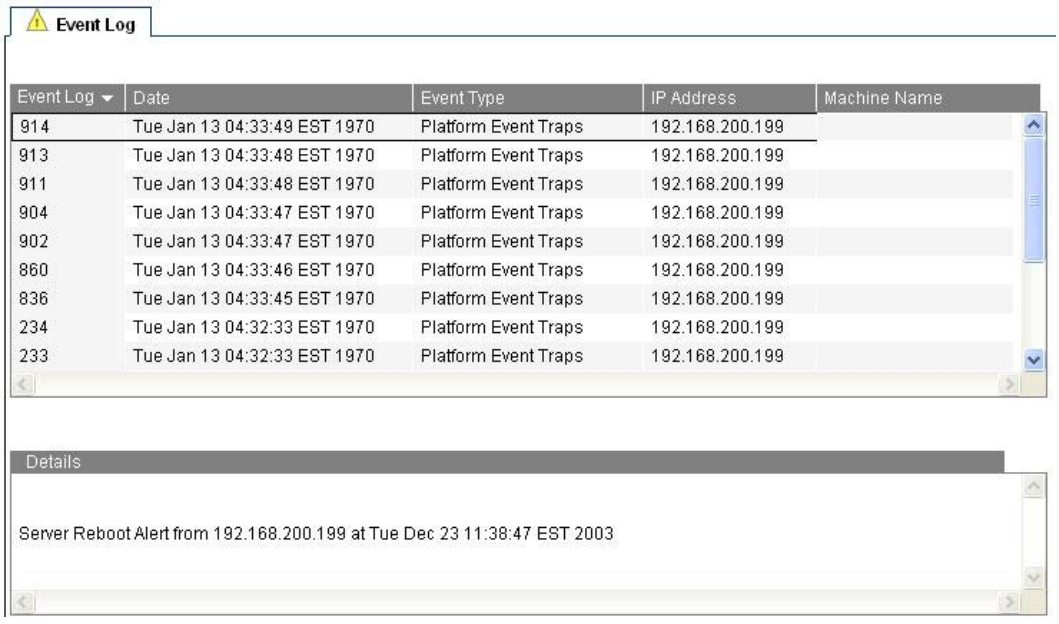


# Chapter 11: Configuring Platform Event Trap Support

System Area Manager is able to receive SNMP alerts in the Platform Event Trap Format (PETs).

The Baseboard Management Controller (BMC) that performs the IPMI management is able to issue SNMP traps when a physical sensor event occurs. The SNMP Trap is formatted to a Platform Event Trap (PET) standard. System Area Manager is able to capture these PETs and notify the central administrators via a chosen notification method designated in the Central Alert Matrix. System Area Manager converts the SNMP trap information into a simple description of the event, providing the administrator with information to identify which server sent the event, as well as the type and severity of the event.

In addition to being notified about the PET, System Area Manager stores the complete SNMP Trap information within its Event Log for later review.



## PET Sensor Types Supported:

-Temperature
-Voltage
-Current
-Fan
-Physical Security
-Platform Security
-Processor
-Power Supply
-Power Unit
-Cooling Devices
-Memory
-Boot Error
-OS Critical Stop

**Note:** If the PET received is not recognized, the administrator will be notified that an unidentified PET has been received and the trap detail will be stored in the event log. ***For more information on PET 1.0 specification please refer to the DMTF Website www.dmtf.org.***

## Configuring System Area Manager to Receive Platform Event Traps

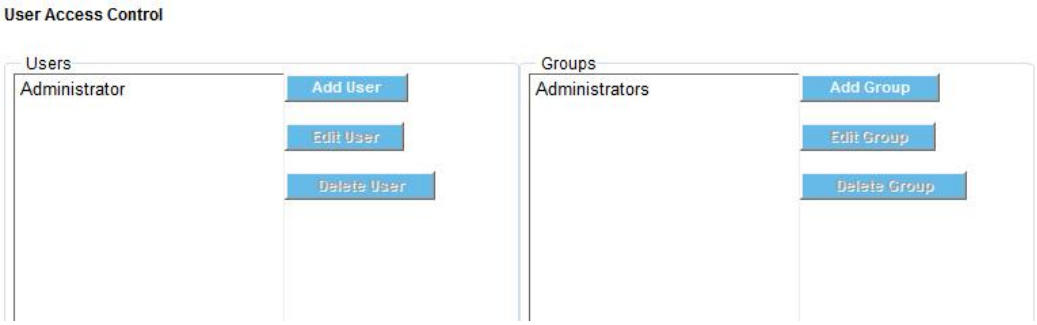
In order for System Area Manager to receive and process PETs, the system must have its SNMP service properties changed to include the community name “Public” and with no other SNMP Trap service running, including the SNMP Trap Service that is automatically installed with the Windows SNMP option.

# Chapter 12: Managing Users and Groups

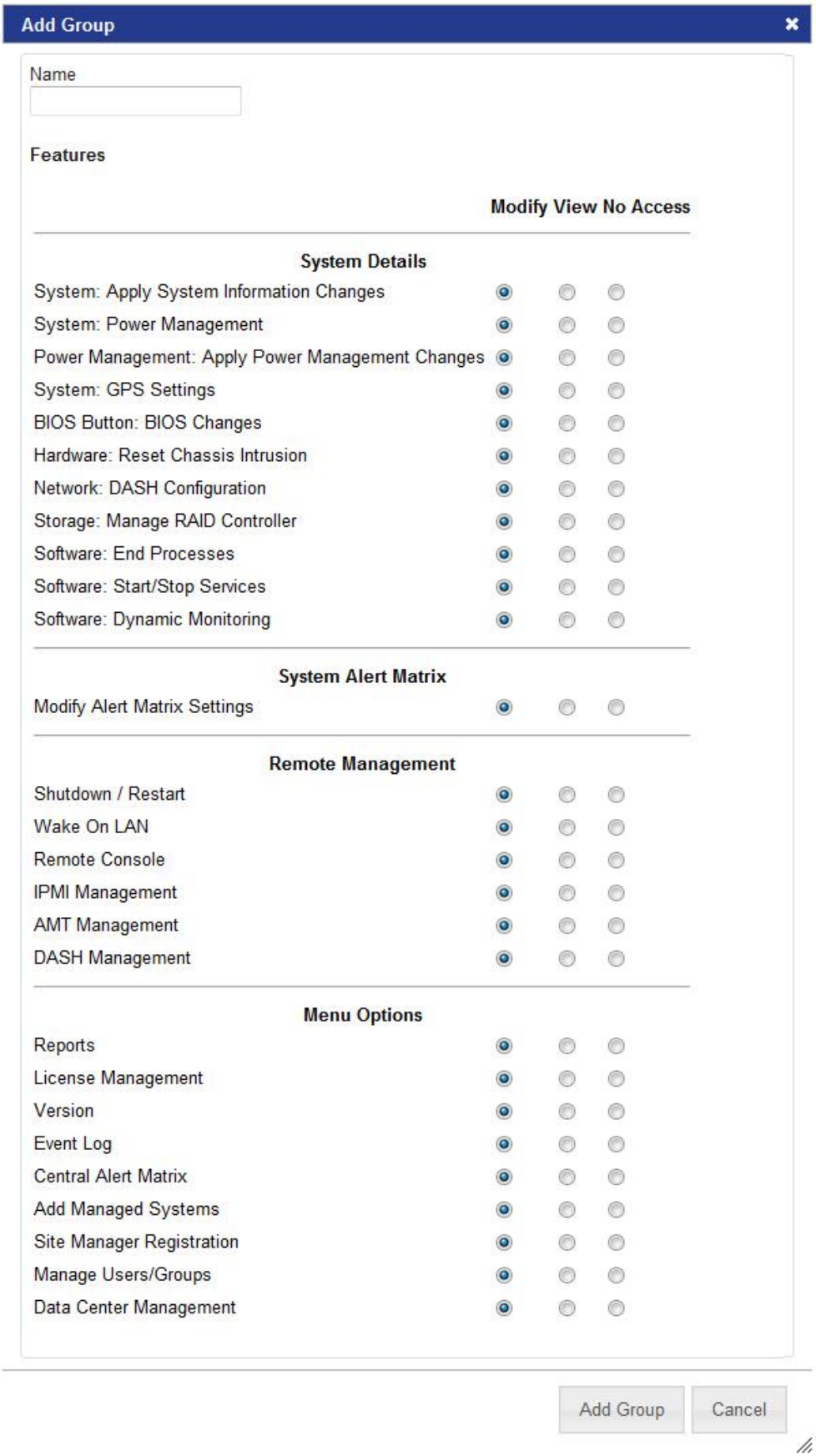
With Version 4.46, users who log into the System Area Manager interface can be given full access to a particular feature, or be allowed to view a setting but not to change it, or have no access to a particular area of the interface.

As in previous versions, login is based on Windows authentication. A username and password used to log into System Area Manager must be a valid login either to the local system of the server running System Area Manager, or to the Active Directory domain to which the server belongs. The local user must have Administrator rights on the system; the Active Directory user must have Domain Admin rights on the Windows domain.

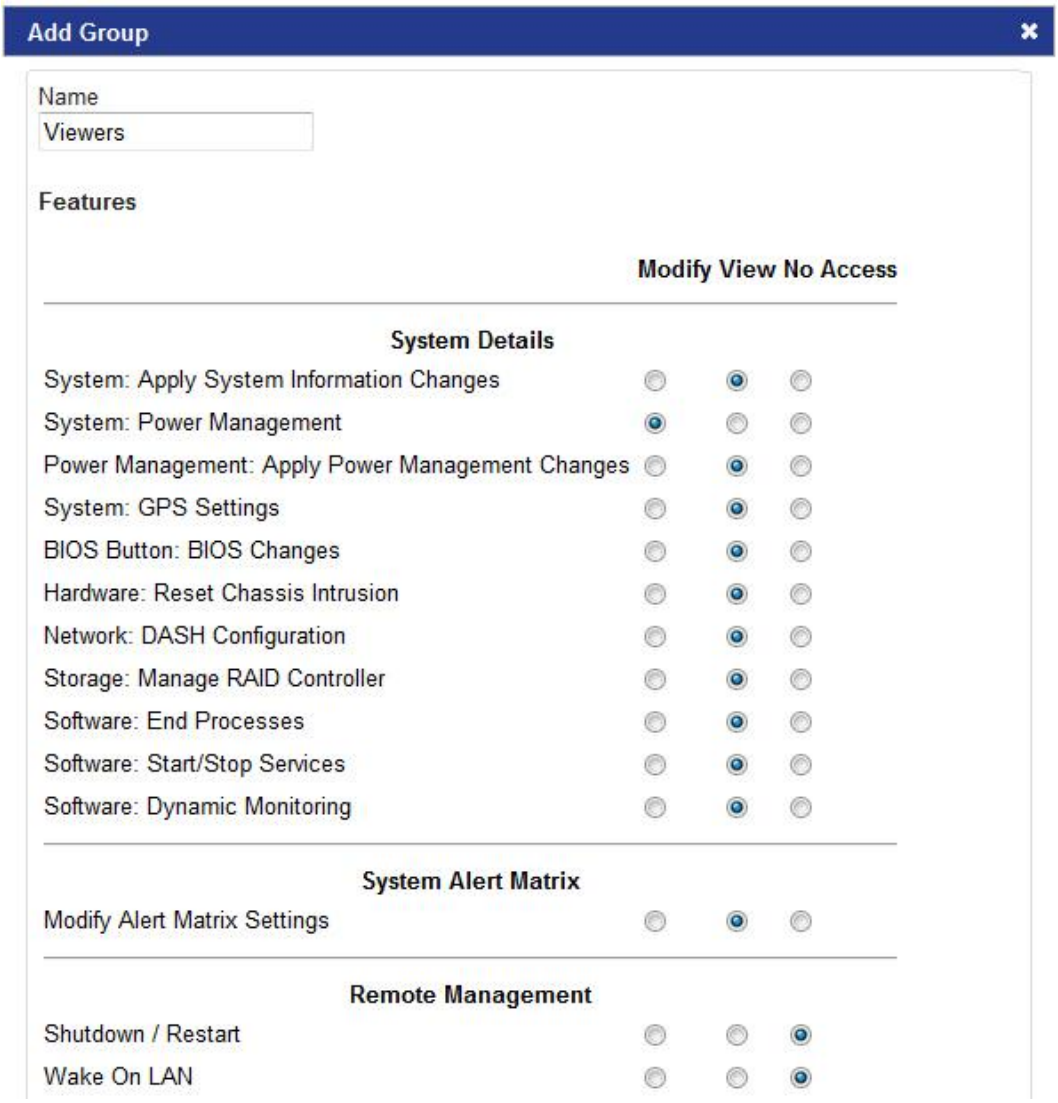
The first user logging in after a fresh installation of System Area Manager, or after an upgrade from a version earlier than 4.46, will automatically be added as a System Area Manager user and will be assigned to the administrators group, for which all available privileges are enabled. All other users must be added in Manage Users and Groups.



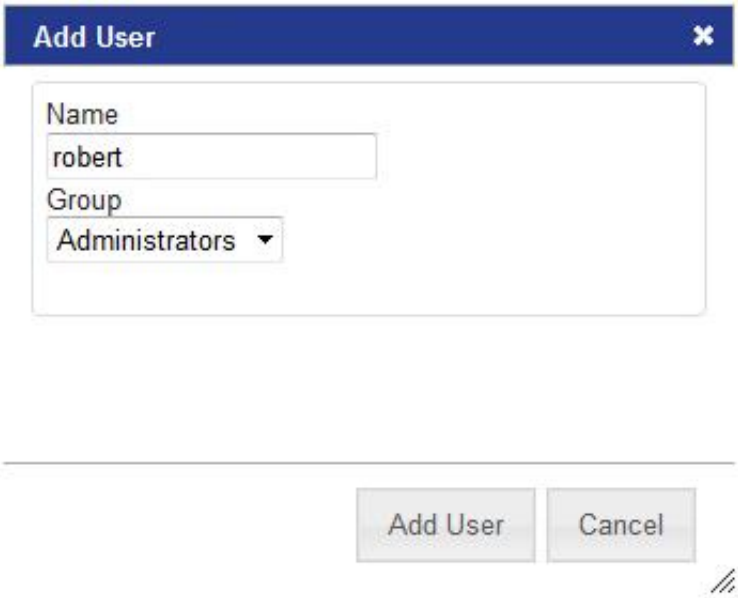

Click the Add Group button to create a new user group.


Add Group
Name
Features
Modify View No Access
System Details
System: Apply System Information Changes
System: Power Management
Power Management: Apply Power Management Changes
System: GPS Settings
BIOS Button: BIOS Changes
Hardware: Reset Chassis Intrusion
Network: DASH Configuration
Storage: Manage RAID Controller
Software: End Processes
Software: Start/Stop Services
Software: Dynamic Monitoring
System Alert Matrix
Modify Alert Matrix Settings
Remote Management
Shutdown / Restart
Wake On LAN
Remote Console
IPMI Management
AMT Management
DASH Management
Menu Options
Reports
License Management
Version
Event Log
Central Alert Matrix
Add Managed Systems
Site Manager Registration
Manage Users/Groups
Data Center Management
Add Group
Cancel

Enter a name for the new user group, and select which features the group's users will be able to use (Modify, View, or No Access).



When adding a new user, enter the username and select the group to which the user will belong.

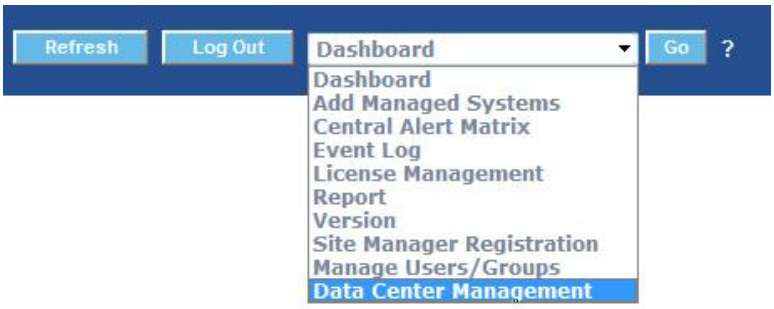



Remember that all users must be valid Windows users, on the server's local system or on the Windows domain.

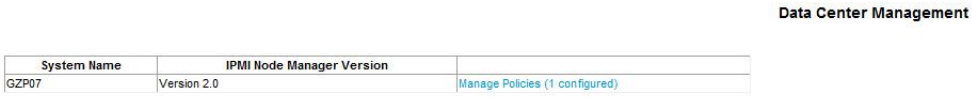
At least one user must belong to the administrators group. To insure that there is a user with full access to all features, settings for this group cannot be changed.

# Chapter 13: Data Center Management

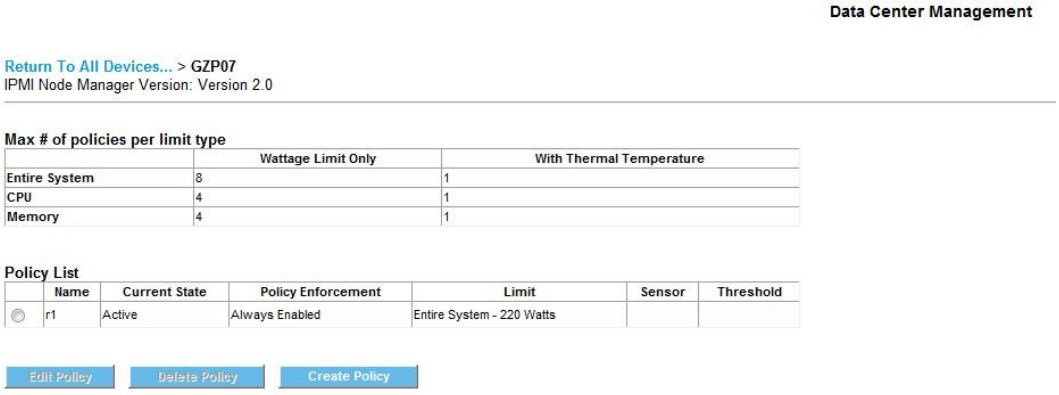
The Data Center Management feature of System Area Manager can be used for supported systems with IPMI Node Manager 1.11 or 2.0. To access this feature, select Data Center Management from the drop down menu.




Click the blue link to manage policies for the supported system.

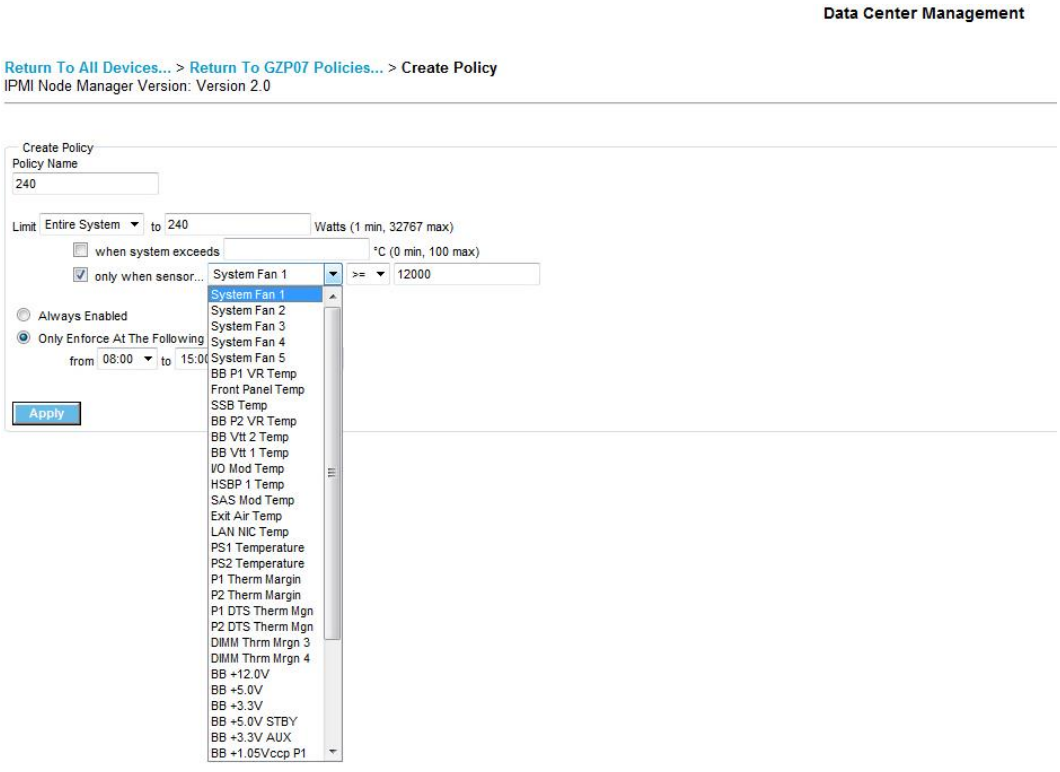



Currently defined policies for the selected system are listed.




Click the Create Policy button to add a new policy.

Enter a name for the new policy. Check the box to apply the limit only when a particular sensor exceeds a threshold value. Select from available sensors using the drop down menu, select the operator (either greater than or equal to, or less than or equal to) and enter the numeric value.




You may configure the policy to be Always Enabled, or click the radio button to limit the hours it is enforced. Select the start and end of the time range, and choose every day, weekdays, or weekends.

When finished creating or editing a policy, click Apply to save changes and return to the list of policies for the selected system. You may have up to eight policies for a system, so you can tailor the system wattage settings as necessary by creating multiple policies.

To edit or delete a policy, click the radio button for that policy, then click the Edit Policy or Delete Policy button.

Return To All Devices... > GZP07
IPMI Node Manager Version: Version 2.0

**Max # of policies per limit type**

| | Wattage Limit Only | With Thermal Temperature |
|---|---|---|
| Entire System | 8 | 1 |
| CPU | 4 | 1 |
| Memory | 4 | 1 |

**Policy List**

| | Name | Current State | Policy Enforcement | Limit | Sensor | Threshold |
|---|---|---|---|---|---|---|
| ○ | r1 | Active | Always Enabled | Entire System - 220 Watts | | |
| ◉ | 240 | Active | 08:00 - 15:00 (Every Day) | Entire System - 240 Watts | System Fan 1 | >= 12000.0 |

Edit Policy | Delete Policy | Create Policy

# Chapter 14: Contact Details & Glossary

## Contact Details

| | |
|---|---|
| Contact | product-support@syamsoftware.com |
| Web | www.syamsoftware.com |
| Support Information | http://www.syamsoftware.com/ |
| Product Information | http://www.syamsoftware.com/ |

## Glossary

**Adding a sensor to the alert matrix**
Sensors are automatically monitored. They have their sensor category default notifications applied to them.

**Asset-monitoring event**
Discrepancy in the systems physical and software inventory.

**Central Alert Matrix**
Administrators use this screen to define the notifications for all of the managed systems.

**Central Alert Notification Settings**
Notification and configuration details for the Central Alert Matrix.

**Central Management Tree**
Displays in a tree format all of the managed systems.

**Changing Central Management Tree grouping**
Click on the <Group By> drop down menu to group systems by Location, Function, or Operating System.

**Changing Central Management Tree sorting order**
Click on the <Sort By> drop down menu to sort by IP address or Machine Name.

**Changing to which System Area Manager the system reports**
Remove the system from the first System Area Manager tree to stop the system from reporting. Once this is done, add the system to the second System Area Manager tree by following the instructions “Add Managed System”

**Critical Level**
The level of the threshold which is operating beyond the normal and warning thresholds.

**Current Value**
The actual reported sensor reading for the system component on a timed reporting cycle.

**Email #1/ #2**
Primary and secondary administrator email addresses

**Event Log**
Record of all of the managed systems events.

**From Address**
Administrators can define a unique name for the SyAM alerting email address.

**Graceful shutdown**
Shutdown a managed system remotely if the agent on that system is in a functioning state.

**Grouping systems**
Group managed system by location, operating system, or function.

**Hardware Detail Screen**
Information on the system components being monitored, including fans, temperature, voltages, etc.

**Hardware Event**
When a threshold is met or exceeded by a physical component of the system.

**Header Bar**
The header bar within this browser contains the **<Logout> <Refresh> <?>** function buttons

**Health colors**
Green = Fully Functional
Amber = Warning threshold exceeded
Red = Critical Threshold exceeded
Grey = System update pending
Blue = Agent has been manually stopped
Purple = System is no longer responding
Black = System has been shut down
Brown = System power state has been suspended

**Intervals**
Readings on all monitored systems and components are at preset cycles of 60 seconds.

**IPMI Event Log**
Hardware event log stored within the IPMI based server

**Logical Sensor**
Storage, network adapters, removable disk drives, and CPU and memory usage.

**Login**
Administrators must login using a user name and password that has administrative rights to the machine that is running SyAM software

**Lower threshold**
The lowest threshold to be alerted upon if it is exceeded.

**Network Detail Screen**
Information on network adapters and their configuration.

**Network Event**
Network connectivity is lost.

**Notification Settings**
Email, SMS/pager, System Area Manager, Network Messages and SNMP Traps.

**Performance utilization event**
CPU or memory utilization threshold is met or exceeded.

**Physical Sensors**
Physical Security, Fans, Temperature, Voltages and Power Unit sensor monitored
**Platform Event Trap (PET)**
SNMP formatted trap received from IPMI-enabled server

**Remote Management**
Shutdown, Reset, Wake on LAN and Remote Console. IPMI Over LAN, AMT Remote Management

**Remote Console**
The Remote Console provides the capability of taking control of a managed systems local screen, keyboard and mouse directly through the web browser from the System Area Manager Interface.

**Removing a sensor from the System Alert matrix**
To remove a sensor it must be in a critical state, then click on the “X” to permanently delete this sensor from the alert matrix.

**Removing systems from System Area Manager Tree**
To remove a system from the System Area Manager Tree, select the system and click on the X.

**Reset period**
The frequency of notifications sent after the initial alert has been sent and if the sensor has not been corrected.

**Restore Physical Sensor Thresholds**
This will reset to the original sensor threshold values when you click on this button.

**Sample period**
Time that is used to take CPU and Memory utilization samples.

**Sensor Status Change back to normal**
When a sensor returns back to within its operating threshold range.

**SyAM Agent**
Non-intrusive monitoring agent configured and managed by the SyAM System Area Manager

**SyAM System Area Manager**
Provides monitoring and communications with all managed agents

**SyAM System Client**
Non-intrusive monitoring agent that can be browsed to directly or managed and configured from the SyAM System Area Manager

**SyAM System Client Tree**
Browsing directly to a system running SyAM System Client.

**SMS Pager #1/#2**
Primary and secondary administrator SMS/Pager addresses.

**SMTP address**
Mail system address: example: mail.company.com or 192.168.1.100

**SNMP Traps**
Notification from a System Client or System Area Manager to an enterprise framework server. Requires System Area Management (SyAM) MIB to be installed on enterprise framework server.

**Software Detail Screen**
Information on the processes, services, and applications installed.

**Storage Detail Screen**
Information on physical and logical disks, controllers and removable devices.

**Storage Event**
Logical disk has reached its utilization threshold, Loss of logical disk, or Loss of Physical disk.

**System Absent**
When the System Area Manager is no longer able to communicate with a managed system, it is reported as being absent, unless it was correctly shutdown.

**System Alert Matrix**
Interface to configure sensor thresholds and notification options.

**System Alert Notification Settings**
Notification and configuration details for the System Alert matrix.

**System Detail Screen**
Information on the system's configuration, BIOS, operating system, location, memory, CPU, etc.

**Upper Threshold**
The highest threshold to be alerted upon if exceeded.

**User name and Password for outgoing Authentication**
Enter the administrator user name and password (if the outgoing email system requires authentication)

**Version**
Displays the Revision and contact details for the product.

**Wake on LAN**
Power up a WOL-enabled managed system.

**Warning Level**
The level of the threshold that is operating between the normal and critical thresholds.